JOANNA ALDERDICE

PRIVACY AND THE INTERNET: *HOW TO RESCUE THE FLY FROM THE TANGLED WEB?*

LLB(HONS) RESEARCH PAPER
MEDIA LAW

LAW FACULTY
VICTORIA UNIVERSITY OF WELLINGTON

2000

CONTENTS

ABSTRACT

The last few years have seen the rise of the Internet as an everyday tool used by millions across the world. This unique medium poses numerous threats to the privacy of consumers, threats that many are oblivious to. The aim of this essay is to expose these problems and explain and critique current systems of protection. The initial issue addressed is whether industry initiatives are effective or whether some form of government intervention is required. The conclusion reached is that current self-regulatory measures leave large areas of privacy unprotected and are unlikely to amount to sufficient protection.

Therefore the main purpose of this essay is to provide a comprehensive and feasible system that Governments could implement to safeguard privacy rights. Blocking the development of such a system is the ephemeral nature of the Internet with its lack of geographical borders. This reduces the ability of local laws to control privacy breaches. What is proposed is a solution via harmonisation, that is conforming laws relating to privacy and the Internet to a basic international standard. Complete harmonisation is admittedly unlikely but if a data restriction provision is enacted the agreement could still be effective.

These international principles must be adequately enforced on a national level. The option advocated is based on the Privacy Commission model already established in New Zealand, and various other countries. This system would allow for industry involvement followed, in appropriate circumstances, by recourse to a privacy agency. In rare circumstances claims could be brought before the courts. The aim of this paper is to provide a practical and useful framework that will protect privacy on the Internet.

The text of this paper (excluding contents page, footnotes, bibliography and annexures) comprises approximately 17,000 words.

I. INTRODUCTION

In a recent case US Navy Petty Officer Timothy R McVeigh sent an e-mail to a volunteer regarding a toy drive for the families of sailors on the navy vessel Chicago. McVeigh sent the e-mail under his America Online ("AOL") screen name "boysrch". Using AOL's member profile directory the volunteer learned that "boysrch" described himself as a member of the military whose marital status was gay. The volunteer forwarded this information to the navy, whose investigators called AOL to ask for "boysrch's" real name. Despite the fact that the investigators did not have a warrant, or even identify themselves, an AOL representative identified McVeigh. The Navy then commenced an administrative discharge proceeding against McVeigh for "homosexual conduct".[1]

This example clearly illustrates that while the Internet may be a "veritable milestone in human evolution"[2] it carries with it a potential cost - the sacrifice of privacy.[3] Approximately fifty million people currently use the Internet and the numbers are expected double by 2002.[4] In survey after survey Internet users cite privacy as the most important issue facing the Internet today, and over three-quarters would go online more often if they felt their private information and communications were secure.[5] It is therefore becoming increasingly important to develop a coherent, practical framework to protect privacy on the net.

To adequately protect privacy, and determine instances of its breach, the first step must be to define what the term means. In cyberspace, as in the physical world, there is

---

[1] It was later held in the District Court of Columbia that the Navy's actions were illegal under the Electronic Communications Privacy Act of 1986. This Act regulates the interception of private communications and access to, and disclosure of, stored electronic communications. McVeigh's career, however, was effectively over and he agreed to retire in exchange for full benefits and payment of legal fees. *McVeigh v Cohen* 983 F Supp 215 (DDC 1998). This case was noted in Eric J Sinrod and Barak D Jolish "Controlling Chaos: the emerging law of privacy and speech in cyberspace" (1999) Stan Tech L Rev 1.

[2] Robert C Vreeland and Bert J Dempsey "Toward a Truly Seamless Web: bringing order to law on the Internet" (1996) 88 (4) Law Library Journal 469, 470.

[3] A simple definition of the Internet is that of a global network that "links together a vast number of computers and computer networks by means of private and public links to provide computer users with access to phenomenal amounts of data worldwide". Clive Davies "Law and the Internet" [1995] 11 (4) Computer Law and Practice 106.

[4] Bryn Williams-Jones "Re-framing the Discussion: commercial genetic testing in Canada" (1999) 7 Health L J 49.

[5] Graphic, Visualisation, & Usability Center (GVU), 8th WWW User Survey (October 1997) P11 at <http://www.gvu.gatech.edu/user_surveys/survey-1997-10/>; Heather Green et al "A Little Net

confusion as to what privacy is and the term is often used to refer to different concepts.[6] This paper will review the area of privacy known as informational privacy.[7] While there is no consensus on the meaning of this term a useful definition that is widely accepted is "the right of individuals to determine when, how, and to what extent, they will share personal information about themselves with others".[8] In general, personal information should only be used with an individual's consent. The purposes for which the information was obtained should determine its subsequent use and disclosure.[9]

Personal information, as defined in section 2 of the New Zealand Privacy Act, is information about an identifiable individual. Some data may be considered more sensitive than others but not only "private" information is included within this concept. It might be that certain types of private information, such as medical details, should be subjected to a higher standard of protection. However, a minimum level must be provided to all information that is linked to an individual. Online privacy often deals with information that is personal without being private.[10] Even innocuous data can be compiled and matched to create a broader picture of individuals that is invasive of privacy.[11] For example address, phone number, income, property value and marital status have always been available for those willing to put time and effort into searching.[12] However, when this data is combined together and is easily accessible, privacy concerns are obviously raised.

Clearly the Internet also provides other opportunities for privacy violations. For example, the sending of "spam" (unsolicited e-mail) may be viewed as an invasion of

---

Privacy Please" (March 16, 1998) Business Weekly Online P3 at <http://www.businessweek.com/1998/11/b3569104.htm>.

[6] Robert A Reilly "Conceptual Foundations of Privacy: looking backward before stepping forward" (1999) 6 Rich JL &Tech 6.

[7] There has been doubt amongst some that data protection is even a privacy issue. Aldhouse convincingly refutes this proposition in "Data Protection, Privacy and the Media" (1999) 4(1) Communications Law 8, 10-11; John Angel also notes that data protection is a form of privacy in "New Rights to Privacy" (1998) 3(5) Communications Law 169, 172.

[8] Michael Power "Bill C-6: Federal legislation in the age of the internet" (1999) 26 Man LJ 235, 238. Alan Westin has adopted a similar definition but includes groups and institutions within its ambit. Alan Westin "Privacy and Freedom" (Bodley Head, London, 1970) 7.

[9] Charles Morgan "Employer Monitoring of Employee Electronic Mail and Internet Use" (December, 1999) 44 McGill 849; Beth Givens, "Symposium on Internet Privacy: privacy expectations in a high tech world, opening presentation" (May, 2000) 16 Computer and High Tech LJ, 347.

[10] Karl D Belgum "Who Leads at Half-time: three conflicting visions of Internet privacy policy" 6 Rich JL & Tech 1.

[11] Steven C Carlson and Ernest D Miller "Public Data and Personal Privacy" 16 Computer & High Tech LJ 83, 87.

[12] Belgum, above n 10.

the recipient's privacy in their home. Such violations are beyond the scope of this essay.

As Part II explains the Internet poses unique challenges to this informational privacy. Most Internet analysts have focussed on the privacy concerns surrounding the controlling of storage, manipulation, and dissemination of information. While these aspects are clearly important controlling the collection of the information in the first place is often overlooked. This initial collection is emphasised in this paper because it is probably of even greater practical importance as it is most amenable to regulation. [13]

This paper aims to determine whether the problems elucidated in Part II are best addressed by state-controlled regulation of the Internet by governmental or quasi-governmental authorities, or through a system of self-regulation by the industry. At the forefront of this regulatory debate is the conflict between the United States (US) and the European Union (EU) in regards to the level of protection that personal information should attract.[14]

Part III therefore discusses the merits of a self-regulatory system of privacy protection. In doing so the organisations that collect personal information and therefore can control, restrict, or affect access, to that information are, and must be, the primary focus.[15] Previously this would have meant concentrating on the government, because it was the only organisation that collected information about individuals on a large scale.[16] Although concerns about government infringement of privacy rights retains its importance, the focus of privacy concerns on the Internet is largely placed on the private sector.[17] Currently, the greatest sources of information on Internet users are private entities, such as clearinghouses and list brokers.[18]

---

[13] Dorothy Glancy "Symposium on Internet Privacy: at the intersection of visible and invisible worlds, United States Privacy Law and the Internet" (May, 2000) 16 Computer and High Tech LJ 357, 361.

[14] David Bender and Danice M Kowalczyk "Avoiding Intellectual Trespass in the Global Marketplace: encryption and privacy in e-commerce" (2000) 2 VA JL & Tech 2.

[15] Reilly, above n 6.

[16] Power, above n 8, 236.

[17] Glancy, above n 13, 377; Jennifer McDermott "Privacy: an overview of recent English law developments" (1998) 3(5) Communications Law 163.

[18] Seth Safier "Between Big Brother and the Bottom Line: privacy in cyberspace" (Spring, 2000) 5 Va JL & Tech 6.

The view of the industry is that their self-regulatory initiatives are, or have the best potential to become, effective protectors of privacy. In the United States this view has largely succeeded. While piecemeal legislation aimed at specific industries has been implemented the primary means adopted for privacy protection is self-regulation.

Is the industry's view correct, are self-regulatory measures effective? The conclusion reached is that while there are merits to these market initiatives important areas of privacy are not protected.[19] The view supported is that of European Commission Director General John Mogg who believes that "self-regulation is a way towards achieving adequate levels of protection" but that it is unproven[20] and not a comprehensive solution.

The inadequacy of self-regulatory measures leads to the need for an effective alternative. Part IV explores other forms of protection that are either indirectly, via the courts, or directly, via legislation, controlled by the state. If an individual chose to bring a claim before the courts there are currently a variety of criminal, tortious and contractual remedies available in varying situations. However, even without the extra problems added by the Internet the courtroom is an ineffective means of protecting privacy.

Does legislation and state-backed enforcement provide a better solution than self-regulation? In contrast to the US the EU has adopted a rigorous approach to informational privacy protection via government enforcement. The conclusion reached is that a legislative scheme similar to that adopted by the EU must be put in place to effectively protect privacy. Legal provisions are needed to define, limit, and protect privacy.[21]

There is, however, a major obstacle in the way of an effective privacy protection scheme based on legislation and state control. The non-existence of a global legal and regulatory framework for Internet privacy protection[22] creates serious jurisdictional hurdles for any country attempting to enforce its law. Part V concludes that to ameliorate these problems there must be a harmonisation of international law on

---

[19] Belgum, above n 10.
[20] Will Rodger "No Privacy Embargoes for Now" ZDNet News March 17 1999 at <www.zdnet.com>.
[21] Belgum, above n 10.
[22] Bender and Kowalczyk, above n 14.

Internet privacy. To provide such a comprehensive system there are two major issues that must be resolved, which are explored in Part VI. Firstly, there must be clear and certain rules to determine which country has jurisdiction over the dispute and whose law will be applied. Secondly, it must be decided when Internet Service Providers (ISPs)[23] should be held vicariously liable for privacy breaches.

Finally, there must be a means of enforcing the legislative principles of the international agreement. This enforcement mechanism is provided in Part VII. A system similar to that of the current Privacy Commission model in New Zealand is advocated. Under this system user complaints would be referred first to the data collector. If the user is unsatisfied he or she could take the action to a further body and then to a tribunal or a court. What is shown is that self-regulatory measures with legislative backing can work together, they are not diametrically opposed to each other.

II. WHY THE INTERNET POSES SUCH A THREAT TO PRIVACY

One may ask why there needs to be a different regime in place to protect personal information on the Internet as opposed to that already present for the real world. The reason is the new ways by which the Internet can hamper the ability of individuals to control their information.

A. Collection

First, and most importantly, there is the risk posed by collection of information from users surfing the net. Website traders collect large amounts of information openly, via such means as forms and surveys, often for the supposed purpose of registering an individual.[24] Arguably consumers could protect themselves by choosing not to fill out the form, supplying false information or abstaining from using the service. Opt-in or opt-out forms might be provided so that the individual could theoretically prevent the collection of information.

---

[23] The definition of an Internet service provider used is that provided for in the Online Copyright Infringement Liability Limitation Act 1998 (US), that is "a provider of online services or network access, or the operator of facilities thereof". This broad definition includes providers of Internet access, commercial on-line services, and operators of individual computer bulletin boards. s12(k)(1)(B)

[24] Including information such as name, address, billing details, and credit card numbers. John Angel "Legal Risks of Providing Services on the Internet" (1996) 1(3) Communications Law 105, 106.

A problem with all of these options is that as the cost of exit grows many consumers will find it harder to avoid the use of certain goods or services.[25] This runs counter to a fundamental requirement of information privacy protection, that meaningful consent to collection must be obtained.[26] This cost is growing because products and services are increasingly becoming contingent. That is, if the information holder does not provide the required information, or allow for its collection, access to sites or products will be denied.

For example, I received this warning when trying to disable the cookies used by Yahoo.Com "Your login has expired. If you do not accept the cookies set on your login or your computer is not configured to accept cookies your session will expire almost immediately. We use cookies to assist us in user authentication and in saving configuration information". On the Internet users often therefore have little choice but to disclose the information to utilise the service.[27]

Via this traditional method of collection the individual is at least aware that data is being collected and might have the opportunity to either consent to, or thwart, such collection. Of even greater danger is information collected covertly without a user's consent. Websites can access information about you simply because you visit their website. ISPs have the ability to monitor the use of services by subscribers to trace, for example, their buying habits.[28]

A common means of covert data collection is via cookies.[29] Cookies are small text files placed on users' hard drives that web sites can use to capture and track clickstream data. Unless a user is knowledgeable enough to set their browsers to notify them about the

---

[25] Reilly, above n 6, para 120. Opt-in and opt-out forms are also flawed for a number of other reasons, as is discussed in Part III.

[26] Leslie A Kurtz "The Invisible Becomes Manifest: information privacy in the digital age" [1998] 38 Washburn Law Journal 151, 169.

[27] David J Klein "Keeping Business out of the Bedroom: protecting personal privacy interests from the retail world" (1997) 15 Journal of Computer and Information Law 391, 393.

[28] Angel, above n 24, 106.

[29] Givens, above n 9, 353. List agents and push technology are a further, more voracious, means of obtaining information. The more you use an agent the smarter it gets. Agents take note of such things as a user's reading material and correspondence, including the most frequent e-mail addresses. They memorise every piece of data and compare and contrast it to the next. In strong form, agents will memorise and process every mouseclick and purchase. Some agents remain on a server while others roam around cyberspace looking for information. Push technology, like agents, revolves around customer profiles. The user sets a profile and the push program does the rest. Each time the user logs on an identifier trips off a certain profile and the program starts collecting content and advertising according to that user's profile. Safier, above n 18.

pending placement of a cookie it is an invisible process.[30] Usually when this transaction generated information is collected the user has already been through some form of traditional information collection.[31] Unbeknownst to the user, data from the cookies on the user's hard drive can be combined with the personal information volunteered.[32]

In fact, various hardware and software systems assign unique identifiers to each personal computer, therefore they can identity and track the users.[33] For example, Real Networks[34] allegedly surreptitiously monitors people's listening habits, and certain other activities, and reports that information to RealJukebox – along with the user's real identity.[35] This is not unusual, 48% of direct marketers actively mine the membership rosters of major online services for information.[36] Even many health-related sites, such as those selling AIDs medicine, collect information from their users and disclose it to third parties.[37]

There is an enormous potential for abuse as these unique identifiers are linked with the real identity of the user and could reveal any kind of information.[38] Service providers might also have access to users' e-mail, where all types of personal information may be provided, and the facilities provided under which subscribers can create their own private databases.[39]

B. Storage and Processing

Compounding these collection problems are the unique storage and processing capabilities now available. With each new application, registration, or transaction, the body of information grows[40]

This problem is exacerbated in the private sector as centralisation is occurring at an alarming rate. The industry has tended to move towards oligopoly and commonly (and

---

[30] Givens, above n 9, 353.
[31] Safier, above n 18.
[32] Toralf Noeding "Distance Selling in the Digital Age" (1998) 3 (3) Communications Law 85, 90.
[33] David H Flaherty "Some Reflections on Privacy and Technology" (1999) 26 Man LJ 219, 220, 226.
[34] A popular RealJukebox software.
[35] Eric J Sinrod and William P Reilly "Cyber-Crimes: a practical approach to the application of Federal computer crime laws" (May, 2000) 16 Computer and High Tech LJ 177, 186.
[36] Safier, above n, 18.
[37] Givens, above n 9, 355.
[38] Noeding, above n 32, 90.
[39] Angel, above n 24, 106.

increasingly frequently) these private actors buy and sell information lists, archives, and databases. Information from both public and non-public sources, from the online and the real world, could be combined to create one giant database.[41] Even information that has been available for a substantial length of time, from either private or governmental sources, becomes more available when readily accessible via the Internet and new databases can be constructed linking the information.[42] Detailed profiles of individuals are available because of this growth of the capacity of intelligent software.[43]

When linked with identifiers the digital records being created pose a great risk to individual privacy.[44] It must be borne in mind that access to this personal data may not just be a threat to privacy but to personal safety. For example, men might be able to locate their battered spouses who have fled or stalkers might be able to locate their victims. The availability of identifying data can also facilitate the misdeeds of others. Criminals, for example, could use this information to perpetuate fraud. [45]

Even more likely, however, is that employers, insurance companies, law enforcement officers, or the Government could use this knowledge to make biased decisions on information that previously would have been unavailable. They can increase their knowledge about your personal activities. Employers, for example, might be able to access records showing an employee, Julie, has visited sites which advocate certain sexual orientations, or unpopular political viewpoints. Julie might then be fired on the basis of that information, or denied promotional opportunities.

Inaccuracy or unfairness might be captured, enhanced, repeated and distributed to create continuing damage and distress.[46] The information about Julie's proclivities might be sold to various entities and become known to potential customers, potential employers, family and so on. These privacy problems are exacerbated because the Internet allows for information to be captured at various locations by diverse means. For example, when Julie visits a website both the systems operator of that site, as well as her own systems provider, can monitor her activity. The data may be stored indefinitely and

---

[40] Safier, above n 18.
[41] Safier, above n 18.
[42] Kurtz, above n 26, 155.
[43] Flaherty, above n 37, 226.
[44] It is clear that employers' collection and use of personal information also raises important concerns however, the focus of this essay is on Internet consumers' information protection.
[45] Carlson and Miller, above n 11, 86.

caching[47] results in the creation of many copies of web pages that are not even under the control of the web site creator. Updates, corrections, and removals will not be reflected on cached copies that can survive for years.[48]

As well as enabling such potential abuse the consequences of human error are magnified in such an environment.[49] Unfair decisions may be made on the basis of inaccurate data. For example, a bank might refuse a loan to Julie on the basis of incorrect information, obtained from a list broker, stating that she was bankrupt.

C. Dissemination

It is not denied that these databases can, however, be beneficial. Benefits to consumers include enhanced efficiency, for example by avoiding repeated screening and authentication,[50] and allowing people to, for example, find lost relatives. It is the policies for disbursing this information that have failed to keep this information secure and have often not restricted use of the information to the purpose for which it was given. It is assumed that McVeigh, for example, would never have consented to AOL releasing his true identity to the Navy.

Large amounts of personal information may be easily accessed and transmitted worldwide within seconds.[51] The time and expense of accessing such information has been substantially decreased or virtually eliminated. Information might be directly used or sold to other companies, mainly to direct marketing services.[52] With the commercial value information now has, there is a heightened chance of trading in confidential information.[53] For example, in America government agencies make significant amounts of revenue via the sale of records.[54] Illinois receives $10,000,000 a year from records sales and Rhode Island raises nearly half that by selling motor vehicle records alone.[55]

---

[46] Simon Chalton "Aspects of Privacy in Relation to Computers" Auckland District Law Society, October 1994, 7.2.

[47] Caching is the creation of an extra copy of a file or files, usually to make them more easily retrievable by the computer user. This can occur on the user's computer or other server computers. Kurtz, above n 26, 157.

[48] Kurtz, above n 26, 153.

[49] Timothy Miller "Law, Privacy and Cyberspace" (1996) 4(1) Communications Law 143.

[50] Safier, above n 18.

[51] Givens, above n 9, 353; Power, above n 8, 236.

[52] Sinrod and Jolish, above n 1.

[53] Miller, above n 49, 146.

[54] Kurtz, above n 26, 155.

[55] Belgum, above n 10.

D. Conclusion

In the online environment consumers often have their ability to control information about themselves impaired or removed. Either users have little choice but to provide information due to the high cost of exit, or information may be taken from them without their knowledge. Once information collection has occurred the user has virtually no control over how it may be used. With huge databases combining personal information being created, and personal information being traded and sold, privacy on the Internet is placed at serious risk. In the words of the Chief Executive of Sun Microsystems "You already have zero privacy – get over it".[56] For these reasons there must be guidelines regulating when information can be collected and what can occur once collection has occurred.[57]

III. SELF-REGULATION

A. Types of Regulation

Worldwide, different forms of regulation, providing different levels of data protection, have been utilised. The focus of this Part is on self-regulation, but following is a brief outline of these various measures to place self-regulation in context.

1. Licensing

Under licensing schemes each data controller must apply to a central authority for a license to collect and/or use data. Licenses might be granted for certain categories of data but may not include others. Data controllers periodically pay a fee for the license. The licensing authority has the power, in certain circumstances, to revoke the license. This would have a severely negative impact on the controller. Such a system was adopted, for example, in Sweden. This means was seen as appropriate as the use of personal identification numbers was widespread and the Government[58] clearly had the ability to link personal data between different files. Licensing was seen as the best means of protecting citizens against privacy invasions.[59]

---

[56] John Markoff "Growing Compatibility Issue: computers and user privacy" *New York Times*, New York, America, March 3 1999, A1.
[57] Kurtz, above n 26, 157.
[58] At the time the Act was enacted the Government was the main focus of privacy concerns as it was the largest collector of information in Sweden.
[59] Greg Tucker "Frontiers of Information Privacy in Australia" (1992) 3(1) Journal of Law and Information Science 63, 64.

These systems are expensive and unwieldy. This is enhanced in the Internet context where both public and private sectors, and entities of all sizes, collect information and would have to register and receive licenses. Currently there is little support for such initiatives. Sweden itself is moving away from this model and towards a notification and registration scheme.[60]

2. *Notification and registration*

Under these schemes the data collector must notify a central authority of the personal files it has collected or is using. Unlike a licensing scheme there is no need for a positive assessment of any application. The collector can continue until otherwise advised by the authority.[61]

This was the form of protection adopted by the United Kingdom's (UK) Data Protection Act 1984 which provided for mass registration and gave the registrar the ability to deregister data controllers. Only a handful of countries adopted the UK's lead towards registration and this scheme has now been replaced.[62] In Ireland the Data Protection Act 1988 provided a registration scheme that was restricted to specific areas of sensitive data which were seen to warrant extra protection.[63]

Registration schemes subject the central authority to a lighter burden and require less administration than a licensing scheme. They have, however, still been criticised for the high compliance and administration costs involved in registering, as well as the complexity of these regimes. It is for these reasons that registration was rejected in New Zealand.[64] These same factors would make a worldwide registration system unfeasible.

3. *Passive schemes*

In these less formal schemes the data protection authority promotes adherence to data protection principles amongst data controllers. Data controllers do not have to record details of the personal files they hold with the authority. The authority must use its

---

[60] Tucker, above n 59.
[61] Tucker, above n 59.
[62] Noeding, above n 32, 91.
[63] Tucker, above n 59, 65.
[64] Privacy Commissioner *New Privacy Protection – Discussion Paper No 12* (Auckland, 1997) 19.

power of persuasion, its own investigations, or public complaints, for its effectiveness. The cost of this model to data controllers and the state is less than licensing and registration schemes. Sanctions may, or may not, be provided. For example the New South Wales scheme only gives the committee an investigatory and reporting role. It has no enforcement capacity.[65]

New Zealand's system falls within this category. A wide definition is adopted of those that must comply with the privacy principles, including any person, company or Government department, with important exceptions. The Privacy Commissioner has a range of functions including monitoring legislation, issuing codes of practice, and investigating complaints. Sanctions are provided, such as damages, costs, orders, and declarations. Systems with such sanctions may be better described as "reactive" rather than "passive". This model is further discussed in part VII. These schemes and self-regulatory measures are really the only two feasible options for cost-effective protection of privacy.

4. Self-Regulation

Self-regulation usually involves encouragement of data controllers by their Governments to adopt good data protection practices. Occasionally internal guidelines or codes of practice are developed within industries as a sign of good faith.[66] Initiatives that are undertaken under Government supervision but not under the direct regulation of Government are included.[67]

The US falls within this last category of protection. There is no agency committed to protecting privacy, and laws vary amongst states. The legislative approach has been described as ad hoc and sectoral.[68] Most legislation has broadly dealt with the regulation of various entities that deal in personal information, such as the credit industry.[69] However, the private sector has by and large not been targeted. This is problematic because, as previously mentioned, private organisations are heavily

---

[65] Tucker, above n 59, 65.
[66] Tucker, above n 59, 66.
[67] Margot Priest "The Privatization of Regulation: five models of self-regulation" (1997-8) 29 Ottawa L Rev 233, 250.
[68] Scott Killingsworth "Minding Your Own Business: privacy policies in principle and in practice""(Fall, 1999) 7 J Intell Prop L 57, 77. For example: The Driver's Privacy Protection Act 1994; Electronic Communications Privacy Act 1994; Right to Financial Privacy Act 1994. For further examples of such legislation see Debra A Valentine "Privacy on the Internet: the evolving legal landscape" (May, 2000) 16 Computer and High Tech LJ 401, 407.
[69] Bender and Kowalczyk, above n 14.

involved with information collection and use. Furthermore most regulation has focussed on the use of the information, versus collection or storage. At best only piecemeal protection is afforded.[70]

Despite this piecemeal legislation the most favoured form of protection online in the US is industry self-regulation.[71] It is the means advocated by the Federal Trade Commission (FTC),[72] various groups and scholars[73], and the industry itself.[74] The Clinton administration has favoured industry self-regulation while supporting the private sector in developing privacy regimes.[75] Self-regulatory measures can form the basis of a FTC action, if a website engages in deceptive acts or practices. However, the FTC cannot require websites to post privacy policies or to prescribe their content. If the website says nothing, instead of misrepresenting what it will do, it does not fall under the FTC's authority.[76] In reality there is little regulation of data collection and use on the Internet.[77]

Why is legal regulation shunned? The main argument is based on the inability of legislation to control information flows. Statutes are seen to have only a limited capacity to protect information in a forum with no geographical boundaries.[78] Self-regulatory initiatives do have the advantage of inevitably being established internationally due to the worldwide operation of communications companies.[79]

Self-regulation can be seen as favourable due to its flexibility to cope with increasing technological innovation and the constantly changing Internet environment. These industry initiatives, it is argued, are advantageous because they are made by those with the greatest expertise and sensitivity to Internet practices. It has also been claimed that

---

[70] Safier, above n 18.
[71] Bender and Kowalcyz, above n 14.
[72] See "Self-Regulation and Privacy Online: a Federal Trade Commission report to Congress" at <http://www.ftc.gov/os/1999/9907/privacy99.pdf>
[73] Such as Peter Huber.
[74] This is the view taken by the Electronic Frontier Foundation and the Computer Professionals for Social Responsibility who favour almost complete exclusion from governmental intrusion. Killingsworth ,above n 68, 77; Reilly, above n 6, para 140-1.
[75] Kurtz, above n 26, 171.
[76] Killingsworth, above n 68, 61.
[77] Givens, above n 9, 350.
[78] Thomas A Lipinski "The Developing Legal Infrastructure and the Globalisation of Information: constructing a framework for critical choices in the new millennium Internet – character, content and confusion (2000) 6 Rich JL and Tech 19.
[79] GUIDEC (General Usage for International Digitally Ensured Commerce) at <http://www.iccwbo.org/guidec2.htm>.

as self-regulatory measures are voluntarily adopted compliance will be broader and enforcement more prompt than when a legislature imposes its mandate.[80]

Looking at the problem cynically, probably the most attractive point in favour of self-regulation from the Government's perspective is that the industry bears the costs. Politically, a Government can reassure critics that the area is being regulated, while taking no direct responsibility for the regime.[81]

As part of this self-regulation different market based initiatives have been implemented and industry advocates claim that such protection is adequate. This essay advocates the principle of individual autonomy – the ability of the user to choose what information is collected, to determine how that information will be used, and to know what information is held about them. Does self-regulation adequately enable individual autonomy?

B. Information Collection

As noted, this stage is the most amenable to regulation as it may be the only time at which the data subject is directly involved and has the ability, if informed adequately, to assert his or her rights.[82] What means has the industry advocated as enabling the user to control and protect the privacy of their information?

---

[80] Valentine, above n 68, 412.
[81] Priest, above n 67, 269.
[82] Belgum, above n 10.

1. Opt-in versus opt-out provisions

At the most elementary level is the debate between opt-in and opt-out provisions. Under an opt-out method the default position is that the information may be collected and used unless the customer indicates otherwise. This is the dominant form of information collection as it is the industry preferred approach.[83] Websites, who want user information for a variety of purposes, have a vested interest in using opt-out provisions and making the default terms of the contract relatively inaccessible. The incentives flow against opt-in provisions.[84]

Opt-out provisions are, however, unsatisfactory. At the time information is collected the user has a right to be fully informed. This includes knowledge of, for example, the fact that information is being collected and the intended recipients of the information.[85] Users may not be aware of the default terms and conditions of their privacy. It is also difficult and time consuming for consumers to locate and comply with the opt-out.

If an opt-in form is used the user may decide if they wish their information to be collected and used, which enables some form of user control and consent. Opt-in provisions are one avenue that might give the user some control over collection. Unfortunately even if this specific consent is given it is often difficult to establish the boundaries of that consent. [86] For example, did that individual consent to having that information combined with previous data? Was the sale of that data to third parties assented to? It is also difficult to apply these ideas of notice and consent to information obtained without the user's knowledge. These covert collection methods would have to be substantially changed for opt-in provisions to be effective.[87]

A problem for both opt-in and opt-out provisions is the increasing cost of, as exit noted above. If the cost of exit becomes too high the consumer is left with no real choice but to provide the information requested. It is clear that consent is meaningless if consumers must consent to receive the benefit or service.[88] A further problem with

---

[83] Reilly, above n 6, para 120; Kurtz, above n 26, 170.
[84] Walter A Effross "Commercial Profiles or Suspect Classifications?: preparing, preventing and parrying public and private profiling" (1999) Stan Tech L Rev 9.
[85] Privacy Act 1993, Principle 3 (NZ).
[86] This is noted in the Australian Privacy Charter 1994.
[87] Kurtz, above n 26, 170.
[88] Reilly, above n 6, para 120.

both types of provision is that a fundamental issue is left unresolved, what happens if the collector disregards its obligation?

2. Technological solutions

There are technical measures available that might enhance privacy protection. These measures are touted by the industry as giving the consumer the ability to protect their own privacy if they choose. This essay is not concerned with a detailed analysis of such protection therefore only the main forms will be briefly discussed.[89]

One such measure is anonymity. If users are aware that information is going to be collected they can visit an anonymising site when login first occurs. For example, Community ConneXion has created an Anonymizer website that shields a consumer's personal information from further websites that are visited.[90] While analysts believe that eventually a suitable formulation will be arrived at for anonymity, currently there are a number of flaws with these forms of protection. Firstly, transactions that occur in cyberspace must eventually link with the real world and therefore the real identity of the user. Secondly, the inability to trace information could reduce the benefits of data gathering mechanisms such as smartcards and agents. Thirdly, the individual must have the ability and knowledge to use such technology and must be aware that information might be collected. If users are unaware information is being collected they will probably not visit an anonymising site. Lastly, the anonymising website knows the true identity of the surfer and could compile it's own user profile, therefore there must be adequate protection against this occurring.[91]

Another common means of protection is encryption. This allows for messages to be sent via the Internet that cannot be read by an outside party.[92] Many businesses use robust encryption to secure information while being transmitted or stored. Many individuals are also utilising encryption to protect their private communications.[93] Software is already freely available on the Internet that produces such strong encryption

---

[89] Other options that might be available include: the use of smart cards to protect identity, active badges, passwords, audit trails and so on.
[90] <http://www.anonymizer.com>.
[91] Reilly, above n 6, 127.
[92] Linda Tsang and others "Focus: e-commerce" Law Society's Gazette (6 October 1999) 96 (38), 25.
[93] Kurt M Saunders "The Regulation of Internet Encryption Technologies: separating the wheat from the chaff" (1999) 17 Journal of Computer and Information Law 945.

that current computers would take millions of years to decode keys that are only a several hundred digits long.[94] However, like anonymity encryption does not help with information that is obtained covertly. Transaction generated information cannot be blocked via encryption.

Looking to the future there are plans for a privacy mechanism to be embedded in cookies and related technologies.[95] However, even if these measures are developed and implemented, as users gain more awareness and better blocking techniques the collection agencies will adopt equal sophistication.[96] Furthermore, to reach a point where any of these measures are acceptable there must be a great deal of consumer education.[97] Hardware and software products that can offer consumers protection must also be easy so that the majority of people can utilise them freely.[98] There must also be consumer trust.[99] To acquire the necessary trust there must be an effective enforcement mechanism in place. Of primary importance is the fact that none of these measures provide for enforcement or protection for the use of information after it has been collected in a decoded form.

3. Open Profiling System(OPS) and Platform for Privacy Preferences Project (P3P)

New protocols are being developed in an attempt to address privacy problems in relation to data collection. These technologies have the ability to both enhance privacy and expand the potential to market information. Both P3P[100] and OPS[101] are examples of

---

[94] One of the safest methods currently available uses a combination of public and private keys. One key is published as an openly accessible directory, the private key is only known to the owner. The OECD has recognised the right of individuals to encrypt their messages. However, in America encryption has been fought against by law enforcement agencies that fear that such technology will be used by terrorists and criminals. A discussion of this issue is beyond the scope of this paper but see: Madeleine Colvin "Covert Policing and the Convention" (1997) 147 no 6820, 1821; Wayne Madsen et al "Cryptography and Liberty: an international survey of encryption policy" (1998) 16 Journal of Computer and Information Law 475;John T Soma and Charles P Henderson "Encryption, Key Recovery, and Commercial Trade Secret Assets: a proposed legislative model" (1999) 25 Rutgers Computer and Tech LJ 97.

[95] Reilly above n 6, para 132 and Kurtz, above n 26, 170-171.

[96] Safier, above n 18.

[97] Reilly, above n 6, para 127.

[98] Reuters "EU Seeks E-privacy Protection" ZDNet News May 21 1999 at <www.zdnet.com>.

[99] Reilly, above n 6, para 127.

[100] P3P is similar to OPS but is in the early stages of development. P3P is being constructed by the World Web Consortium (WWC). WWC is an industry standards group comprised of more than 200 businesses and academic institutions.

[101] See Open Profiling Standard Frequently Asked Questions (May 27, 1997) at <http://www.developer.netscape.com/ops/opsfaq.html>. OPS was created by more than 60 companies, including Netscape and Microsoft. Kurtz, above n 6, 171.

"secure, automated, one to one applications for the instantaneous formulation of legal and social contracts and agreements associated with business processes".[102]

In both examples a user creates a personal profile with his or her information, which at the user's option can be securely stored in a corporate-wide or global directory. The first time that an individual visits a website that supports one of the programmes the website requests information from the personal profile. The individual can then choose to release all, some, or none of the requested information, and can authorise further use of that material without permission. If the website collects additional information it can, with the user's permission, store that information on the profile.[103] In theory the individual can determine the level of privacy that he or she requires.

Significantly these programs will allow for both the expression of privacy practices and a notification system, as well as the secure storage, transport and release of data.[104] Technology such as P3P may ultimately resolve some of the privacy problems - in particular those relating to the collection and security of data. Unfortunately these systems are currently flawed. If, for example, P3P was used the user would be blocked from many sites. This may be unacceptable to consumers. Additionally to use the system a certain level of computer literacy is required to set the preferences to attain the desired level of protection. Furthermore, the future of these measures is far from certain. For example, P3P itself is in doubt. The Consortium failed to release the measure onto the market by its deadline and one of the former Consortium members has filed a patent for the technology.[105]

These measures do not adequately protect information that has been collected. Once the individual releases the Personal Profile to a website there is no technical way to prevent a website from reusing or sharing that information. Websites are therefore encouraged to post privacy policies and consumers are encouraged not to release information if a site does not have one. Again the question must be asked, what happens if the policy is not adhered to? Promises might be disregarded and all of the information might be taken, although this could be alleviated somewhat by encryption,[106] or misused. For a more in depth discussion of privacy policies see below.

---

[102] Reilly, above n 6, para 130.
[103] Reilly, above n 6, para 130.
[104] Reilly, above n 6, para 132 and Kurtz, above n 26, 170-71.
[105] Sinrod and Barak, above n 1.
[106] Reilly, above n 6, para 136-7.

C. Information Use and Disclosure

As noted, information should only be stored, used, and disclosed to third parties, in limited circumstances, such as explicit authorisation, consent at the time of collection, or for law enforcement purposes. For self-regulation to be effective there must be sufficient measures in place to ensure that these principles are adhered to. Are there currently such measures?

1. Codes of practice and privacy policies

Self-regulatory measures commonly take the form of a company's own privacy principles. Sometimes companies adopt trade association codes of fair information practices. Under current US law, companies are at liberty to choose which policies they implement and how to enforce such a policy.[107]

Merely adopting a privacy policy, however, is not enough, it must also be followed. For example AOL, the ISP that released McVeigh's information without his consent, disregarded its own privacy policy. AOL's policy states that "America Online Inc is strongly committed to protecting the privacy of consumers of its interactive products and services".[108] To ensure compliance it is widely recognised that fair information practice codes should contain enforcement mechanisms.[109]

Unfortunately these policies have not been effective. In a recent study over 90% of websites studied were found to collect data from their users. Less than 10% had privacy policies that contained all of the FTC's crucial privacy policy requirements of notice, access, security and third party disclosure.[110] Most policies simply provide notice and opt-out, while ignoring the other principles.[111] The FTC found that websites soliciting personal information, including only those overtly collecting information, usually did

---

[107] For a useful discussion see Peter Schnaitman "Building a Community Through Workplace E-mail: the new privacy frontier" (1998/1999) 5 Mich Telecomm Tech L Rev 177.
[108] AOL.com, Privacy Policy at <http://www.aol.com/info/privacy.html>.
[109] Valentine, above n 68, 407.
[110] The FTC looked for notice, choice regarding data use, access, security and enforcement. Mary J Culnan, Georgetown Internet Privacy Policy Study (July 21, 1999) at <http://www.msb.edu/faculty/culnann/gippshome.html>.
[111] Givens, above n 9, 355.

not contain any posted privacy policy.[112] This is particularly concerning as the FTC standards are not particularly onerous and are not as stringent or as broad as the European protection.

In June 1998 the FTC summarised the problem with industry self-regulation in regards to privacy:

> Despite the Commission's three year privacy initiative supporting a self-regulatory response to consumer privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information trade practice (notice/awareness) ... In addition, the guidelines, with limited exception, contain none of the enforcement mechanisms needed for an effective self-regulatory regime.[113]

A pertinent example of this failure is provided by the Geocities case.[114] Geocities was one of the most visited websites on the Internet. It provided a "virtual community" which offered a variety of services, including free e-mail and clubs, as well as hosting members' home pages. Both mandatory and optional information was requested on its application form. Via website statements, members were assured that the mandatorily provided information would only be shared with third parties for the purpose of providing them with the particular advertising they requested. They were also assured that their optional information would only be released with their permission. The information was in reality being sold or rented to third parties that used it for other purposes.[115] What this example clearly shows is that in reality self-regulation may equal no regulation.[116]

---

[112] Belgum, above n 10.
[113] Federal Trade Commission, "Conclusions" in "Privacy Outline: A Report to Congress" (last modified June 9, 1998)at <http://www.ftc.gov/reports/privacy3/conclu.htm>.
[114] In the matter of GeoCities, a corporation, FTC File No 9823015, at <http://www.ftc.gov/os/1999/9902/9823015cmp.htm>
[115] A case was bought against Geocities by the FTC which was settled via a consent order that prohibited Geocities from misleading its customers about data collection, use or disclosure and from misrepresenting who was actually collecting the personal information. Killingsworth, above n 68, 60.
[116] Tucker, above n 59, 66.

2. Privacy seals and trustmarks

A further privacy enhancing measure, and a form of market self-regulation, is that of privacy seals or trustmarks. TRUSTe is the oldest such initiative and is the leading privacy seal program supporter. TRUSTe[117] gives seals to those websites that adhere to its privacy policy.[118] Websites that obtain the seal must disclose to the consumer and to TRUSTe which information they gather, how the information will be used and who they share the information with. They must also promise to submit their sites to periodic audits.[119] TRUSTe can use technical measures to detect any privacy policy changes that are implemented.[120]

Another example of a trustmark system is the BBBOnLine Privacy Program (BBB) created by the Better Business Bureau. The BBB is intended to compete with the TRUSTe seal. TRUSTe is associated with Internet brands such as Microsoft and Nasdaq while BBB is associated with main street America. The principles at the base of this program are encouraging. The program requires adherence to rigorous principles of notice, disclosure, choice, consent and access. Participants must explain their policies in plain English. On every page that data is collected there must be a link to the privacy policy. This should enable a user to make an informed choice on the collection of information.[121]

Importantly, BBB provides an enforcement system. As noted this is a prerequisite of any effective privacy protection system. The system sets up an arbitration process that consumers can use to protest unfair or deceptive conduct.[122] BBB can also conduct unscheduled inspections of websites. As part of the program the companies agree to provide the restitution that BBB dictates, apart from fines.[123] As punishment BBB could remove its seal or refer complaints to the Federal Trade Commission.[124] Both

---

[117] TRUSTe was founded by CommerceNet and the Electronic Frontier Foundation and began in 1997.
[118] Rodger, above n 20.
[119] Bender and Kowalczyk, above n 14.
[120] Killingsworth, above n 68, 86.
[121] Yinka Adegoke "US Seals Online Custom with Privacy Mark" (April 5, 1999) The Lawyer, Centaur Communications Limited.
[122] Adegoke, above n 121.
[123] Maria Seminerio "BBBOnline Introduces its 'Trustmark'" ZDNet News March 17, 1999 at <www.zdnet.com>.
[124] Rodger, above n 20.

BBB and TrustE could also sue for breach of promises in its licensing contract.[125] BBB will accept complaints against any website, not just those that are part of the program.[126]

BBB has also had some success in membership numbers and coverage. By April 1999 more than 300 companies had applied to become members. BBB also coordinates with local BBBs to provide privacy information and model privacy policies to businesses worldwide.[127] The BBB believes its strong brand recognition outside the Internet will give the seal credibility and help it to grow. The BBB has 270,000 members offline and about one quarter of those have websites.[128]

An obvious advantage of these "seals" is that the cost is borne by the industry itself. The program members pay a licensing fee of between $150 and $3000 depending on their size and corporate sponsors are funding the program's start up costs, by paying between 50,000 and 100,000 dollars.[129] TRUSTe has a similar sponsorship program and its licensees pay between $300 and $5000.[130]

Noeding believes that such schemes, once accepted, will do more for privacy protection than data protection legislation could ever hope to achieve.[131] If money and power back these schemes up they can be effective and enforceable. Unfortunately, to date, only a tiny percentage of companies on the net have actually signed up for such regulation.[132]

The purpose of such initiatives is also problematic. Are these private sector groups acting to protect consumer or industry interests? The problem with these groups monitoring information use and collection is that they are often comprised of industry versus consumer interest groups. The industry's focus is clearly more on the desire for the new currency of information than consumer rights.[133]

Not only are industry initiatives self-interested but they are also likely to display favouritism. That is, they will be dominated by larger companies and will pursue their

---

[125] Killingsworth, above n 68, 86.
[126] Seminerio, above n 123.
[127] Adegoke, above n 121.
[128] Seminerio, above n 123.
[129] The BBB is sponsored by more than 20 global companies.
[130] Seminerio, above n 123.
[131] Noeding, above n 36, 92.
[132] Rodger, above n 20.
[133] Bender and Kowalczyk, above n 14.

own interests – not the interests of the industry, let alone the public.[134] Even Hendricks, author of Privacy Times, believes such programs are not adequate, particularly as there is no assurance that they will be widely adopted. However, he believes that such measures could provide the basis for privacy laws.[135]

3. Voluntary agreements with the Government

In the US a significant number of participants in the online advertising industry have entered an agreement with the FTC as to rules governing the tracking of Web surfers. Online marketers have agreed to refrain from combining online data with offline information banks. They agreed to secure approval first, but only via opt-out provisions. Clearly displayed opt-out provisions so the user can avoid tracking by the marketers must also be provided. A complete ban on using sensitive information has been agreed to. The advertisers must also agree to give consumers access to personally identifiable data and demand that the e-commerce sites they use contractually commit to follow the advertising firm's privacy policy. Enforcement will occur via an industry-funded agency.[136]

What this shows is that federal regulators still believe that self-regulation can be successful. It remains to be seen whether this faith is well-founded. The agreement itself may be criticised as only opt-out provisions are included. These have already been found wanting and affirmative consent should be gained. Again this system doe not provide universal coverage or a general privacy code but only caters for part of one sector, the advertising arena. It is just another part of an already confusing and ad hoc form of protection. Whether this agreement will be adhered to, and whether the enforcement mechanism will be effective, is questionable. The problem with industry based enforcement groups noted above are equally applicable here.

---

[134] Priest, above n 67, 273.
[135] Seminerio, above n 123.
[136] Glenn R Simpson and Jerry Guidera "Online-Advertising Group Agree to Protect Privacy of Consumers' Data" The Wall Street Journal, 28 July 2000.

D. Information Storage

Once information has been collected and stored by the data collector it is relatively easy for that collector to protect the security of the information against most outside interference. Encryption and data security techniques can make Internet information inaccessible as a practical matter.[137] Due to encryption most information sent out can be protected unless up against a dedicated hacker. Firewalls can be used to protect local area networks from unwanted interrogation by outsiders. However, the best security measures cannot prevent privacy invasions if staff are not trained on using the measures or required to follow privacy policies.[138]

E. Cyber-Courts

A word should be said on the approach advocated by certain theorists who support the establishment of a cyber-court to govern the Internet, perhaps even set up within the Internet. It is argued that such a court is better suited to the online environment as it would avoid the jurisdictional problems discussed in part VI. This online forum would also, according to its advocates, be more knowledgable about Internet practices than real-world courts and government agencies.[139]

Johnson and Post argue that cyberspace can create its own law and legal institutions. They believe a consensually based set of rules will emerge from a self-governing community of online users. Those subject to these "laws" would remain free to move among different online spaces.[140] How an online court would work mechanically is not clear. Hardy imagines online cyberspace hearings, with judges, juries and attorneys. The sanction meted out would be expulsion from the relevant part of cyberspace.[141]

In the Internet context a transnational dispute resolution body may soon become a reality for domain name disputes. In 1997 the "Generic Top Level Domain

---

[137] Glancy, above n 13, 364.
[138] Northern Legal Office Exhibition, The Lawyer, October 14 1997, Centaur Communications Limited, 8.
[139] Peter Bartlett "Internet: the legal tangle" [1995] 11 (4) Computer Law and Practice 110, 112.
[140] Johnson and Post "Law and Borders – the rise of law in cyberspace" (May 1996) 48 Stan L Rev 1367.
[141] Trotter Hardy "The Proper Legal Regime for Cyberspace" (Summer 1994) 55 U Pitt L Rev 993, 1053.

Memorandum of Understanding" established a procedure for resolving domain name disputes, which was widely adopted with many signatories from around the world. This was developed by the World Intellectual Property Organisation and a Policy Oversight Committee. A panel of international experts was established to receive petitions from rights holders to determine if the domain name policy has been violated. Included in the system is online mediation, arbitration at the option of the right holder, and Administrative Domain Name Challenge Panels. This system has the advantage of having no impact on national court jurisdiction.[142]

This sort of court might provide an alternative dispute resolution forum[143] and might be viable for arbitration clauses in commercial contracts.[144] However, it is not appropriate for a mainstream communications network[145] that has the potential for large breaches of privacy. According to Trout-McIntyre there are numerous problems with cyber-courts. For example, if the court is to be based on new governing "laws"what happens if these governing "laws" fail to emerge? Johson and Post do not address this problem, rather they take it for granted. These courts would also encourage forum shopping as the user would have another forum in which to bring a suit. Furthermore there are serious problems with judicial tenure and jury accommodation.[146] For such a system to work a great deal of international cooperation would also be required. It is unlikely that a government would acquiesce to this sort of jurisdiction.[147] The creation of cyber-courts would probably therefore "create more problems than they could alleviate".[148]

---

[142] See <http://www.gtldmou.org/presentations/cg-jan22/index.htm>. For a description see Clive Elliott "The Internet – a new world without frontiers" (Nov 1998) NZLJ 405, 408. There are further programs that work with users to resolve conflicts that arise from Internet use, such as the Virtual Magistrate Project and Ombuds Online Project. See Tammy S Trout-McIntyre for a discussion of these initiatives "Personal Jurisdiction and the Internet: does the shoe fit" (Fall, 1997) 21 Hamline L Rev 223, 267.

[143] Bartlett, above n 139, 112.

[144] The Honourable Michel Bastarache "The Challenge of the Law in the New Millennium" (1998) 25 Man LJ 411, 417.

[145] Bartlett, above n 139, 112.

[146] Trout-McIntyre, above n 142, 259.

[147] Bastarache, above n 144, 417.

[148] Trout-McIntyre analyses the establishment of a cyber-court in her article, above n 142, 259.

F. Conclusion

I have reached the conclusion that it is doubtful that a self-regulatory approach will provide sufficient protection, particularly for access and enforcement.[149] The question then raised is can self-regulation become effective? For this to occur there must be sufficient incentives for companies to implement adequate protection or join privacy schemes. As increased privacy would lead to increased Internet business this might provide an incentive. It goes without saying that most private companies are profit driven. There is clearly enormous growth potential for e-commerce and the Internet. By 2002 e-commerce is expected to grow to C$653 billion globally.[150] Many non-users have cited privacy as the most important reason for staying off the Internet.[151]

There are encouraging signs that this concern is motivating Internet data collectors to take action. Currently the so-called "800-lb gorillas" of the online world are throwing their weight behind privacy policies. Last year both IBM and Microsoft, the Internet's two largest advertisers, announced that they would not advertise on websites without posted privacy policies. Disney's "Go Network" went even further and stated that it would not advertise on, or accept advertising from, websites that did not have comprehensive privacy policies.[152] These large corporates have the potential to exert substantial pressure on websites.

However, lack of consumer confidence and negative publicity have so far not proven to be a significant enough incentive for comprehensive privacy protection by the industry. As consumers are currently often unaware of privacy breaches there may be little negative publicity. For example, despite Geocities privacy breaches the site remains the second most popular site for New Zealand surfers.[153] While studies clearly show consumers have fears about their privacy, and that some are refraining from transactions because of this, the volume of online sales and the growth of the Internet is still exploding. Therefore, while consumer concern might be an incentive for some organisations that wish to increase their sales, this is not an adequate incentive for all

---

[149] Kurtz, above n 26, 173.
[150] Fasken Martineau DuMoulin "E-Commerce Canada" International Law Office Nov 1999 at <http://www.internationallawoffice.com/ld.cfm?Newsletters_Ref=1233>.
[151] Belgum, above n 10.
[152] Killingsworth, above n 68, 67.
[153] Nigel Horrocks (ed) *NZ NetGuide* (Industrial Press Ltd, Auckland, 2000) Issue 40, June 2000, 16.

organisations that collect information from the Internet. With the cost of exit increasing there is less chance that consumer confidence will provide a sufficient incentive. Also, not all Internet data collectors are engaged in e-commerce and therefore do not fear bad publicity or a loss of product sales.

Additionally the tangible benefits obtained by the market from privacy breaches probably outweigh the possible negative publicity that may be incurred. Personal information primarily raises revenue. Information can be onsold, traded, used to target services or to attain advertising. Information as to customers likes and dislikes is invaluable in such an environment. A recent study by Cimex found that one out of every 13 jobs in the United States was the result of direct marketing sales activity. The study also found that direct marketing sales to consumers reached $630 billion in 1996, compared to $458 billion in 1991.[154] As the value of personal information skyrockets so does the potential for abuse.

A further incentive might be provided by the industry fear that unless self-regulation is effectively implemented the public might demand the imposition of heavy-handed government regulation.[155] The recent agreement between advertising agencies and the FTC mentioned above was entered into because of such a threat. However, that might be a risk that the industry is prepared to take. Indeed it seems intuitively unlikely that predominantly profit-driven organisations will have the motivation required to enact a sufficiently stringent scheme.

It is acknowledged that solutions to collection problems can be partially provided via technical means. However, these methods are far from foolproof and as it is virtually impossible to suppress information that has already found its way to the web, strong controls and incentives need to be put in place to prevent the misuse of information. The enormous power and potential for abuse held in the hands of Internet data collectors must be kept in mind. McVeigh lost his career over an e-mail and an ISP's disregard for his privacy.

Individual industry initiatives that may not be widely adopted are probably not capable of providing the certainty and clarity required. Even with more websites participating in

---

[154] Such as jobs designing and selling advertising, supplying and selling customer and consumer lists and profiles to direct-response businesses. Safier, above n 18.
[155] Belgum, above n 10.

privacy programs it is a real risk that only a self-selecting pool of Websites will voluntarily agree to regulate themselves.[156] Self-regulation is unlikely to provide an equitable or adequate solution without some form of public governance. When this is coupled with the potential for abuse and the lack of incentives and market success to date it is clear that some form of government enforcement is required.

IV. STATE BACKED PROTECTION

A. Recourse to the Courts: an indirect form of state regulation

There is a currently a confusing array of laws which directly or indirectly have some impact on data protection. There are actions available for such things as breach of confidence, privileged communications, trespass, and the implied contractual duty of secrecy. For example, there have been numerous civil suits filed against plaintiffs allegedly harmed by anonymous Internet postings but the underlying causes of action have varied from defamation to privacy to unauthorised possession of proprietary information.[157] The criminal law has also been utilised to provide limited protection of data, in particular by computer crime legislation.[158]

In theory informational privacy would be protected as tortfeasors would have to pay for the damage suffered and because private lawsuits in conjunction with public scrutiny can motivate information providers to implement and adhere to sufficient privacy policies. However, these laws at best only provide incidental protection[159] and there are glaring inefficiencies inherent in such a liability regime. The confusing number of actions leads to procedural complexity making it hard for consumers to ascertain their rights. This in turn makes it hard for data collectors to establish their responsibilities. This complexity also leads to increased transaction costs.[160]

---

[156] Sinrod and Jolish, above n 1.

[157] David L Sobel "The Process that "John Doe" is Due: addressing the legal challenge to Internet anonymity (2000) 5 VA JL & Tech 3, para 13. Bartlett, above n 139, 110. Cases have also been fought in America over the sale of information to direct mail advertisers without consent *Shibley v Time Inc* 341 NE 2d 337, 339 (Oh App 1976); and the gathering of personal information from Internet users without consent *Newby v Alexa Internet and Amazon.com*, C 00 0054, US District Court, Nortern District of California (filed Jan 6 2000); Double click has also been subject to a similar claim. Reilly, above n 6, para 106.

[158] In the late 1990's in America there were nearly 40 cases on the criminal use of e-mail alone. Samuel A Thumma and Darrel S Jackson "The History of Electronic Mail in Litigation" (1999) 16 Computer and High Tech L J 27.

[159] Tucker, above n 59, 79.

[160] Flaherty ,above n 37, 220.

As with any action it is usually too expensive, stressful, and tedious to have recourse to the courts. A trial will also often involve the further disclosure of personal information. Furthermore significant personal harm is often required. The difficulty this raises for protecting informational privacy on the Internet is that often the damage suffered by an individual is minimal but many people may be minimally injured.[161]

A brief look at the protection afforded by the privacy tort will serve to illustrate this point. Consumers today receive a modicum of protection via the common law doctrine of invasion of privacy.[162] The common law torts fail because they do not protect actions taken in public and the Internet is arguably a public environment.[163] Indeed recourse to legal protection often depends on reasonable expectations of privacy.[164]

This is often hard to establish in a public environment like the Internet. Issues arise as to whether a user reasonably expected privacy when he or she accessed the Internet. Is a chat room, for example, public or private? It is argued by some that if a user sends an e-mail via the Internet that it would be unreasonable for an action to arise as it is commonly known that the Internet is not secure.[165] A further hurdle is that, as noted, much of the information in question while personal is not private. Normally the privacy invasion must also have been unreasonable.[166] It is clear that privacy does not provide significant protection for the offline world let alone the new online environment.

Some countries, such as Britain and Australia, do not even recognise the existence of a common law right to privacy.[167] In fact for any court claim each jurisdiction will have different statutes and common law actions to apply. This disparity leads to complex jurisdictional issues and the potential for forum shopping, which is further discussed in Part VI. Most companies are therefore basically impervious to tortious suits, due to the problems discussed above coupled with the issues raised by cross-jurisdictional transactions. These actions therefore provide little incentive to protect privacy.[168]

---

[161] Lipinski, above n 78.
[162] In New Zealand the common law right of privacy was reaffirmed recently by the High Court in *P v D*. Bell Gully "Media Law" May 2000 at <http://www.bellgully.com>.
[163] See Belgum, above n 10, who provides an analysis of why the four privacy torts rarely apply to online privacy violations. See also Glancy, above n 13.
[164] Glancy, above n 13.
[165] Angel, above n 24, 109.
[166] Glancy, above n 13, 367.
[167] A description of the common law position in England is noted Angel, above n 27, 169.
[168] Reilly, above n 6, para 108.

A Contractual Model?

Would allowing Internet users' informational rights to be determined solely by contract provide a solution? Traditionally personal information has not been viewed as belonging to the information subject.[169] However, ownership and use of information has pointed to the emergence of an Internet regime based on private contract.[170] Contractual entitlements are coming to the fore in the United States. Under this approach the individual would voluntarily disclose personal information in exchange for some benefit, either money or more likely an online credit,[171] thereby forming a contract. Negotiating these exchanges can be quick, easy, and largely cost free.[172]

Market forces and consumer pressure have led to some business entities involved in the collection, storage and use of personal information on the web guaranteeing greater legal protection by offering a sort of quasi-contract that exchanges the use of a service for personal information.[173] These companies are moving towards viewing information as a person's property.

However, the typical problems of imperfect information would apply to such a contractual system. Firstly, there is a lack of consumer education. An uniformed user cannot truly consent to the collection or use of the information. In particular consent is impossible when information is taken surreptitiously. Secondly, there is inequality of bargaining power. Most individual users are not in the position in which to bargain. As noted above, the cost of exit is constantly increasing, making the reality of equal bargaining partners unrealistic. The user wants or needs to use the service or product and currently the provider is in the position to prevent access if information is not

---

[169] Katrine Evans *Privacy and Publicity: restraining abuses of power in New Zealand* (LLM, Victoria University of Wellington) 61.
[170] Lipinski, above n 78.
[171] Examples of authors who have analysed privacy issues from a market perspective are: Richard S Murphy "Property Rights in Personal Information: an economic defence of privacy" (1996) 84 Geo LJ 2381; Paul M Schwartz "Privacy and the Economics of Personal Healthcare Information" (1997) 76 Tex LJ Rev 1; Peter P Swire "Cyberbanking and Privacy: the contracts model" (abstract of talk for computers, freedom and privacy 1997, San Francisco, March 1997) at <http://www.osu.edu/units/law.swire.htm>; Electronic Privacy Information Centre, Report 49-1, Privacy Guidelines for National Information Infrastructure: a review of the proposed principles of the privacy working group at 2(1994) available at <http://www.epic.org/privacy/internet/EPIC NII privacy.txt>.
[172] Reilly, above n, 6.
[173] Reilly, above n, 6.

provided. Lastly there is an inability to tailor agreements for the individual.[174] Without tailored contracts the intention of the user is unclear.

It is acknowledged that contract will to some extent be determinative. There will be situations were there is parity between the user and the information collector and a genuinely negotiated contract. In these cases the contracts formed should be treated no differently to those entered into in a traditional manner.[175] In fact I advocate contractual negotiations between the user and collector in certain circumstances as part of the solution provided in Part VII. However, allowing informational rights to be determined solely by contract would lead to the majority of agreements being "drafted unilaterally by a dominant party and then presented on a 'take it or leave it basis' to the weaker party with no real opportunity to bargain concerning the terms of the contract".[176]

Enforcing contracts across different jurisdictions again raises the sorts of jurisdictional issues discussed in Part VI. Such as, when users are in different countries and form a contract over the Internet where is a contract made? Furthermore, on the Internet often a formal legal contract will not exist but some other level of interaction between the parties will arise.

Regardless of whether such perfectly formulated contracts exist there must still be adequate means of enforcing the contract and controlling the way information is used once it is released. [177] The individual will lose control of their information once it is made public. Even if the terms of the contract prohibit reuse outside of agreed purposes or retransmission of the information to third parties these terms would be difficult to enforce.[178] Therefore a contractual model is not a complete solution to privacy problems and an adequate privacy protection system will still need to be established.

B. Legislation the European approach

As demonstrated in the United States a sectoral legislative approach leads to large gaps where there is little or no privacy protection. In conjunction with various, largely ineffective, self-regulatory measures this leads to consumer confusion. Of more

---

[174] Reilly, above n 6, para 117.
[175] Trout-McIntyre, above n 142, 250.
[176] Lipinksi, above n 78.
[177] Lipinski, above n 78.
[178] Belgum, above n 10.

importance to companies that collect personal information is that consumers do not trust them[179] which actually inhibits the growth of e-commerce and the free flow of information.

However, the failure of this sectoral approach is not fatal to the use of legislation. America's patchwork approach is in marked contrast to the system in place in the EU, Canada, Australia, New Zealand and Hong Kong. In these countries omnibus data protection laws have been enacted that cover "the full spectrum of uses of personally identifiable information".[180] The state plays an active role in providing legislation and enforcement mechanisms.

The European model is an example of a comprehensive legislative approach to privacy. The European Data Protection Directive 1995 (Directive) requires the introduction of statutory privacy controls. It obliges all member countries to adopt national laws incorporating its requirements and takes a rigorous approach to notice, consent, accuracy and access.[181] The implementation of these principles by the EU has been described as "fastidious and rigid".[182]

Through a wide definition of processing the Act regulates virtually anything which can be done with information, from collection to mere holding or destruction.[183] Web sites must tell users about what information is collected and allow users to refuse disclosure. Users have the right to access information held about them and the right to correct it. Users can refuse the sale or sharing of their personal data with online and offline companies.[184] Appropriate exceptions are provided. Those involved in journalistic, literary or artistic activities in certain specified circumstances are exempted from most of the key provisions of the Act.[185]

The Directive presumes data processing is illegal unless certain conditions are met. The unambiguous consent of the data subject is one condition that can make processing

---

[179] Givens, above n 9, 350.
[180] Givens, above n 9, 348.
[181] Kurtz, above n 26, 173. Santha Rasaiah "Current Legislation, Privacy and the Media in the UK" (1998) 3(5) Communications Law 183, 184.
[182] Killingsworth, above n 68, 79.
[183] Rasaiah, above n 181, 184.
[184] Kurtz, above n 26, 173.
[185] These conditions are set out in section 32, see Rasaiah, above n 181, 184.

legitimate.[186] The idea of universal registration was replaced with details of processing carried out depending on the threat processing offers to the subject. The Act covers any information about an identifiable person, whether on computer or in a structured manual file, whether paper based or automated. Particularly tight conditions are imposed on processing certain types of sensitive data.

The security requirement is flexible to allow for technological developments, the measure that must be taken must be appropriate to the risk presented and the nature of the data. There is a particular focus on the transfer of information to non-EU countries. Data can only be transferred to a country that ensures an adequate level of protection.[187] Adequacy is left undefined. On can be "relatively confident" that New Zealand's Privacy Act, for example, is adequate.[188] However the US has not been recognised as having adequate protection.[189]

The Directive must be enforced by a national regulatory body with statutory authority that has wide discretionary powers to implement more detailed restrictions.[190] Individuals in the EU countries also have a right of action; "every person has a right to a judicial remedy for any breach of the rights guaranteed to that person by the applicable national law". The aim is to empower citizens to take action against companies that misuse their data. Member states must provide appropriate sanctions.[191] The EU also requires the availability of private money damages as a form of enforcement.

Such a comprehensive legislative approach is required. What this legislative intervention provides is greater certainty and clarity than either a court based or self-regulatory approach. A baseline of privacy protection must be provided via codification of fair information principles.[192] Clear rules must be set out for individuals as to whether their information can be collected and what rights they have once it has been collected. This would enable individuals to identify breaches so as to exercise the available legal

---

[186] Data Protection Act 1998, s32. For a discussion of this exception see Rasaiah, above n 181.
[187] There are exceptions, such as the unambiguous consent of the data subject. Noeding, above n38, 91.
[188] Discussion Paper No 12, above n 64, 11.
[189] Killingsworth, above n 68, 77.
[190] Rasaiah, above n 181, 183.
[191] Kurtz, above n 26, 173.
[192] Givens, above n 9, 355.

remedies.[193] Legislative backing is required to ensure sufficient coverage of the industry and provide for enforcement sanctions.[194]

V. HARMONISATION

> ***"Incompatible national laws operating upon a single indivisible data flow can (could) only lead to inconvenience, disharmony, ineffective law and, in the end, the dominance of the laws of the most economically powerful jurisdictions".***[195]

It has been argued that Data Protection Acts, such as the Directive, can not effectively address Internet privacy problems because they are unenforceable in that context. There are two reasons for these claims. Firstly, the Internet is global and information can be accessed and collected about individuals from anywhere in the world. The Internet is not based in one country or region,[196] nor is it owned or controlled by one governing body.[197] Secondly, data can easily be transferred from the protected country to "data havens", places where no protection exists.

It is true that due to the lack of geographical boundaries the ability of local laws to control privacy breaches is reduced. It is also true that there is currently no new international law or enforcement mechanism to protect privacy rights on the Internet. Despite this dissolution of boundaries, however, there is the potential, and indeed the necessity, to structure new boundaries.[198] This is necessary because the Internet is subjected to a myriad of legal regimes that make it easier for wrongdoers to avoid detection and prosecution and leads to legal uncertainty and confusion. Additionally if varying standards are in place and liability may arise in different jurisdictions forum shopping will occur - that is, the plaintiff will be able to choose to bring an action in the jurisdiction that is most amenable to the claim.[199] What is required is real international regulation that could ameliorate the inter-jurisdictional problems[200] and would prevent

---

[193] Chalton, above n 46, 7.3
[194] Preist, above n 67, 249.
[195] Hon Justice Micael Kirby "The Globalisation of Media and Judicial Independence" (1996) 1(3) Communications Law 115, 117.
[196] Davies, above n 3, 106.
[197] Bartlett, above n 139, 110.
[198] Lipinski, above n 78.
[199] Davies, above n 3, 109; Bartlett, above n 139, 112.
[200] Kirby, above n 195.

countries from becoming homes for illegal activity.[201] If there is no universal agreement there will be many data havens which might leak information back into the protected country.[202]

What form should this regulation take? What is required is a convention or treaty that addresses applicable law, regulation, jurisdiction, and enforcement to form a standardised environment.[203] What is required is the process of harmonisation, conforming national laws to a basic international standard. Canada's Information Highway Advisory Council has identified this need for bilateral and multilateral arrangements at the international level for Internet abuse.[204] Appropriate principles for Internet privacy protection must be agreed on at an international level. These principles would then be implemented in national legislation.[205]. As in the EU it would be for the national law to determine whether an event is harmful provided that the effectiveness of the international agreement is not impaired.[206]

It has been said that a drawback of harmonisation is that it is in essence the lowest common denominator to information access and control. It is true that a conciliatory and democratic approach may lead to an agreement that is emasculated and compromised. However, this will depend on the strength of those bargaining and the incentives that can be provided for agreeing to higher standards.

Unless the language used is too general and ambiguous the principles could provide both guidance and flexibility. At a national level the use of broadly worded guiding principles has not been seen as fatal. The principles can provide guidelines as to acceptable conduct and provide a basic system that is consistent. In fact it is better to provide a framework of principles to apply to new technology rather than deal with each new technology as it arises by specific privacy laws.[207] In New Zealand there has not been a serious problem with the general principles of the Privacy Act.[208] The international agreement will be most useful if the international community treats it as

---

[201] Reilly, above n 6.
[202] Miller, above n 49, 146.
[203] Jeremy Landau "The Effect of Multi-Media Communication on Jurisdiction and Enforcement" (1996) 1(2) Communications Law 58, 60.
[204] Tanya Schamach "Child Pornography in Cyberspace" (1996) 2 Appeal 58.
[205] Chalton, above n , 7.3
[206] Landau, above n 203.
[207] Privacy Commissioner Bruce Slane "Smart Cards, Privacy and Business Conference" (18 October 1996, Sydney) 1.
[208] Evans, above n 169, 193.

flexible and capable of occasional supplementation as issues require.[209] This avoids the criticism that legislation is too rigid to be practical.

A. Is International Agreement Possible?

I have concluded that it is necessary to move from the current ad hoc regime to a global legal and regulatory framework, but is this possible? A look at current systems governing the international regulation of data or the Internet provides guidance as to the ability of international consensus to be reached on effective information principles.

In the context of general data information protection there appears to be some general consensus as to the principles involved. Many data protection statutes are based on the same principles. There are two international documents that establish the general informational privacy principles at an international level: the OECD Guidelines of 1980[210], the United Nations Guidelines of 1990.

The basic data protection principles propounded in the OECD guidelines and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1980 have influenced, and sometimes precipitated, much of the legislation enacted since 1981 in a number of countries, including Australia and New Zealand.[211] The OECD has also been able to develop new principles under its guidelines for the new Internet environment, for example on the security of information systems and encryption principles.[212] For example, in 1998 the OECD adopted the Protection of Privacy of Global Networks declaration.

The intent is that countries will be assisted in developing policies and regulations and to give guidance on core characteristics to business and consumer groups and self-regulatory bodies. Non-member countries are invited to take account of these

---

[209] David Harland "The Consumer in the Globalised Information Society - the impact of the international organisations" (1999) CCLJ Lexis 10, 15, 33-34.

[210] All twenty–four OECD member countries have adopted these guidelines. However, different forms of implementation have been utilised: thirteen countries have comprehensive data protection legislation covering both the public and the private sector, other countries such as Australia, Canada, Japan and the US only have laws relating to certain sectors; some have enacted no laws at all, such as Belgium, Greece, Italy, Switzerland and Turkey. Tucker, above n 59, 68.

[211] Kirby, above n 195,117; Tucker, above n 59, 69.

[212] Cryptography Policy (1997) and on Consumer Protection in electronic commerce (1998); Noeding, 92; Discussion Paper No 12, above n 64.

guidelines due to the OECD's limited membership.[213] Consensus and a common approach to assure individual control was arrived at which influenced domestic laws.[214]

In regards to Europe there is also the Council of European Data Protection Convention of 1981 and the supra-national instrument the European Union Framework Data Protection Directive.[215] The substance is similar in all of these instruments, although the Directive 95/46/EC elaborates these principles in greater detail. These principles are discussed below.

What this illustrates is that agreement is possible. There are further precedents for international treaties covering areas that are relevant, such as the Berne Convention and the GATTS/TRIPs agreement. If the EU could come to a consensus, for example between Germany with its stricter privacy protection and England with its historical lack of protection, then this provides hope that such an agreement could be reached between other countries.[216]

Who might be responsible for developing these principles? While there are various possibilities the organisation that is probably best placed is the OECD. The OECD is an international regulator that might take the lead in formulating international homogeneous legislation, and might perhaps become a supervisory body. If adequate OECD principles were adopted this could lead to a degree of harmonisation of laws, as well as to effective international self-regulatory schemes and dispute resolution.[217]

The United States continues to dominate the Internet therefore their cooperation in any data protection initiative is essential. Hope is provided as the privacy protection principles advocated by the FTC are not that different, though less strict, than those of the EU. As concerns over privacy increase Congress and the President have become increasingly willing to push for the industry to adopt stronger measures.[218] Even without the cooperation of the US those that sign the agreement could lead the way in privacy protection with the hope that others will follow.

---

[213] Harland, above n 209, 45.
[214] Kirby, above n 195, 117.
[215] There are twelve member countries.
[216] Flaherty, above n 37, 230.
[217] Harland, above n 209, 45.
[218] Sinrod and Jolish, above n 1.

It is acknowledged, however, that a complete harmonisation of laws is virtually impossible. Therefore the EU restrictive transfer provision might provide a way for individual nations or regional blocs to enhance privacy. Under the Council of European Convention Issued Recommendations 1991 the Directive's transfer restriction applies unless necessary measures have been taken to respect the principles. For example, contractual measures reflecting the principles with the data subject having the opportunity to object, or obtaining the data subject's free and informed consent in writing.[219] Most laws based on the OECD guidelines do not have such a restriction.[220]

Unless countries with insufficient legislation can prove that companies can voluntarily protect the data as required by EU's data protection laws even major multinationals could be banned from routine business transactions.[221] If a list of jurisdictions that had adequate protection were compiled this would ease compliance and administrative costs.[222] What the Directive proves is that while a country might not be able to regulate what happens outside its jurisdiction it can control what information leaves its boundaries and enforce its rulings on those within its geographical borders.

B. The Principles

The principles that are at the basis of so many agreements are broadly that personal data shall be: processed (which includes collected) lawfully and fairly; only obtained for specified and lawful purposes with consent and not further processed incompatibly with those specified purposes; adequate relevant and not excessive for their purpose; accurate and if necessary up-to-date; not kept for longer than is required; processed in accordance with the rights of data subjects; provided with security measures against unauthorised or unlawful processing. Within the EU there is the additional principle that data can not be transferred outside the European Economic Area without an adequate level of protection for the rights of data subjects.[223] Underlying these principles is the idea of transparency, provided through consent and notice. [224] These more stringent EU requirements should be favoured over the FTC requirements.

---

[219] Seminerio, above n 123.
[220] Discussion Paper No 12, above n 64.
[221] Seminerio, above n 123.
[222] Discussion Paper No 12, above n 64.
[223] This helpful summary was provided by Aldhouse, above n 7, 9.
[224] Schnaitman, above n 107.

This basic outline is clearly incomplete and many details would need to be worked out. For example, if information is held about an individual within a country, even if they do not reside there, that individual should have rights to access, perhaps with a reasonable charge imposed in appropriate circumstances.[225] Further, the identity of the information collector is not always simple, often the entity for whom the site ultimately collects the data is not revealed.[226] The website should therefore be required to display who it is collecting information for. Companies should also be required to conduct privacy impact assessments on their products and services in the development stage.[227] Appropriate exceptions would obviously have to be included.

When these principles are formulated those involved must be careful to ensure that both the information rich and poor are considered and that the national or commercial interests of one population segment don not supersede citizens' collective rights.[228] What would be required is both consumer and industry input. Consultation must occur with appropriate industry groups such as the World Wide Web Consortium (W3C). The W3C is ideally suited as a non-profit organisation that sponsors committees that look at Internet problems and attempt to determine solutions.[229]

1. Collection

The purpose of this essay is not to provide comprehensive principles. However the principles relating to collection will be explored in more depth. This is because, as noted above, collection is the stage most amenable to regulation and is overlooked by most commentators. The approach adopted is that advocated by Cavoukin and Tapscott, who believe in stringent safeguarding of personal information from the outset.[230] As previously mentioned, what is required is meaningful and informed consent to information collection. The EU requires that the subject has "unambiguously given his or her consent"[231] and Quebec requires that consent should be free, enlightened and given for specific purposes. The consent is only valid for the time needed to achieve the purposes assented to.[232]

---

[225] Privacy Commissioner *A Guide to the Privacy Act 1993 - Discussion Paper Number 3* (Auckland, 1 July 1993).
[226] Belgum, above n 10.
[227] Givens, above n 9, 355
[228] Lipinski, above n 78.
[229] Noeding, above n 32, 92.
[230] Reilly, above n 6.
[231] European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 24 October 1995, Article 7(a).
[232] "Protection of Personal Information in the Private Sector 1993" s14 (Quebec Act).

If consent is to be meaningful and real choice is to be given to the consumer the choices must be easy to make and the consumer must be adequately informed as to the availability of the choice and its implications. The Hong Kong Personal Data (Privacy) Ordinance 1995 includes the following principle that should be implemented:

> "*Information to be generally available*
>
> All practicable steps shall be taken to ensure that a person can:
>
> (a) ascertain a data user's policies and practices in relation to personal data;
>
> (b) be informed of the kind of personal data held by a data user;
>
> (c) be informed of the main purposes for which data held by a data user are or are to be used."[233]

Limits should not, however, purely be implemented at the point of data collection from the individual but should extend to data obtained from public records and third party sources.

The Hong Kong section applies to information that is not collected directly from the individual and generally requires agencies to be open about their data policies and practices. The principle should not be linked to collection as much information is indirectly acquired. This not only gives the user choice but also facilitates access and correction.[234] As in New Zealand, information should only be collected for a lawful purpose connected with the function of the agency.[235]

2. A differing standard for sensitive information?

Some data categories might be regarded as more sensitive than others and therefore deserving of differing protection. The EU Directive requires additional safeguards for sensitive information.[236] Certain data must be subject to opt-in clauses, such as that relating to religious and political affiliations and medical conditions. For all other personal information there must be an opt-out clause.

Is this an appropriate distinction? I would argue that, at least on an international level, it is not. Sensitive information is hard to define and varies with different cultural

---

[233] Schedule 1, principle 5. Noted in Discussion Paper No 12, above n 64.

[234] These are some of the benefits listed in the Australian Privacy Charter in regards to their openness principle.

[235] Agency includes any person, company, or government department, with some important exceptions.

[236] Article 8.

settings. Such measures would need to be at the discretion of each jurisdiction. Importantly, there is the risk that sensitive categories might be emphasised to the detriment of good information practices generally. The system might also become more complicated leading to increased administrative and compliance costs.[237]

To avoid confusing distinctions all information should be subject to opt-in clauses. This would give individuals greater control over the use of their information.[238] As noted, the problem with these opt-in provisions is that they do not fit well with covertly obtained information. What must be addressed is the collection of information not just via active means but also through passive means, such as cookies. If such covert means are used this should be noted and a link should be provided to a page that provides instructions for disabling the means of collection.

While the information that must be provided may appear onerous it is possible for Web sites to develop and display, for example, standardised logos which would indicate what sort of privacy protection is provided and who can obtain the user's personal information.[239] In the model advocated below the Privacy Commissioner could develop these logos. If collectors displayed these logos but did not follow the measures they stand for enforcement action could follow.

It has been said by the Direct Marketing Association that these provisions would be "death to us ... If you can't use information about a person without permission, that generally means you're not going to have a list of great substance".[240] However, individuals have a right to control information about themselves. Information collectors are profiting from users' information and therefore should take on responsibilities. Marketers receive direct benefits while at best consumers only receive indirect benefits in the form of services that are targeted to their tastes. Opt-in clauses would not kill the marketing industry, rather marketers and information collectors would have to provide incentives for information provision. These incentives could include reduced rates, free services, or promotions to those willing to provide their information.

---

[237] Discussion Paper No 12, above n 64, 16.
[238] David J Klein "Keeping Business Out of the Bedroom: protecting personal privacy interests from the retail world" (1997) 15 Journal of Computer and Information Law 391, 408.
[239] Effross, above n 84.
[240] Robert S Greenberger, Mass Marketers Say High Court Ruling Will Boost Costs, Mean More Junk Mail, Wall Sreet Journal, Jan 18, 2000 at B8.

These incentive systems must, however, allow for real consumer choice. If those who do not provide the information can not use the service that essentially negates any consent that might be given. The proposed Canadian Charter contains a right that has no equivalent in the New Zealand Privacy Act, it provides that there is a "duty not to disadvantage people because they elect to exercise their rights to privacy".[241] What needs to be recognised is that the individual has the right to decide whether or not to release their information and how that information should be used, not the data collector. Maybe an ISP could offer two prices, with a higher one for those who refuse to release their information.[242]

Allowing for the user to remain anonymous, if they choose, is important. Using Internet services on an anonymous basis may be the most effective means of preserving privacy. The right to anonymity has been recommended by the House of Commons in Canada[243], and has been included in the US National Infrastructure principles[244] and the Australian Privacy Charter[245]. This right has been limited by phrases such as remaining anonymous "when appropriate" and identifying individuals only if it is "reasonably justified".

It must be borne in mind that only personally identifiable information is restricted. Statistics, for example, of how many people visit a certain website or buy a certain product that are not linked to an individual are perfectly acceptable. Furthermore, broadly speaking, the purposes for which information is collected can be broadened or narrowed, as long as the user is adequately informed, has a real choice and consents thereby forming a contract.

---

[241] Recommendation 2, clause 5.1

[242] Rochelle Cooper Dreyfuss "Warren and Brandeis Redux: finding (more) privacy protection in intellectual property law" (1999) Stand Tech L Rev 8, 27.

[243] "Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified."
Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: where do we draw the line?*, Ottawa, April 1997, recommendation 2.

[244] "*Empowerment principle*
Individuals should be able to safeguard their own privacy by having ... the opportunity to remain anonymous where appropriate."
Privacy Working Group Information Policy Committee Information Infrastructure Taskforce, "Privacy and the National Infrastructure: principles for providing and using personal information", 6 June 1995.

[245] "*Anonymous transactions*
People should have the option of not identifying themselves when entering transactions."

C. Are there Sufficient Incentives for such a Harmonised System to Become a Reality?

Initiatives such as those taken by Europe and the OECD are the only way forward to prevent the loss of informational privacy on the net.[246] However, the failure of the EU and the US to reach agreement despite extensive negotiations and the threat of data restrictions indicates the difficulty of trying to establish a harmonised system. Harmonisation clearly provides benefits for consumers but are there sufficient incentives for the state to implement such a unified system?

At the moment Internet developments are occurring virtually outside of government regulation thereby depriving the state of autonomy in this area. The state's ability to control data collection is exacerbated by the global nature and ephemeral nature of the Internet, and the problems this leads to for national enforcement. States may be more likely to compromise their sovereignty than to altogether lose any semblance of control.[247] Pressure from consumers and their advocate groups might also have an impact. As time progresses, with more people using the Internet and instances of privacy breaches becoming more apparent, pressure will probably increase.

Under harmonisation the current confusing array of statutes, common law, and self-regulatory measures can be avoided. One of the advantages of harmonisation is that it provides fairness. Similar acts in different places will produce similar results. If a uniform system were implemented Internet data collectors and service providers would have clear guidelines to operate by. If they complied with the relevant laws would not be held liable.

From a purely commercial viewpoint there are sufficient benefits to the government, and the industry, to become involved in a harmonised system. Universal fairness is economically efficient.[248] With uniform regulation the simplicity of businesses operating across jurisdictions and assuring with compliance will decrease costs.[249] A major benefit is that personal data in identifiable form and for commercial purposes can be moved between signatory countries without any form of privacy protection scrutiny

---

[246] Harland, above n 209, 33-34.
[247] Harland, above n 209, 21.
[248] Lipinksi, above n 78.
[249] David Kerr "The Case for Regulation" GuardianUnlimited 20 April 2000 at <http://www.huardian unlimited.co.uk/freespeech/article/0,2763,212474,00.html>.

because each of the members have equivalent, comparable privacy protection.[250] This eliminates the transaction cost of negotiating agreements between information sellers and buyers in countries that comply. A harmonised approach also facilitates access as some producers are reluctant to offer their information products and services to citizens in countries that have not adopted adequate protection.[251]

The biggest incentive is probably that "the country that best updates its legal framework to facilitate e-commerce will gain a comparative economic advantage".[252] If system administrators worldwide had to work to ensure the security and integrity of their systems consumer confidence would increase and more online business would be obtained. There is a larger likelihood that users engage in electronic commerce. In contrast to this a lack of harmonisation and the consequential fear of a milieu of divergent policies may inhibit the growth of the Internet and in particular e-commerce. While this has not been a noticeable problem so far as more divergent legislation is enacted and courses of action are established the risk is increasing.[253] Industry and Government both therefore have a vested interest in providing for safe trading.

Data restriction provisions could also provide incentives to the harmonisation of law, they are not restricted to achieving mere diplomatic pressure[254] The importance of the EU in international trade has caused countries to revisit, and revise, their laws. Countries with consistent legislation could form blocks of power made up of those with consistent legislation. These large blocks could then place pressure on smaller blocks or states to try and force them to comply.

Under a harmonised system with a data transfer restriction if a country does not have adequate legislation transfer should not necessarily be barred to the entire country. Transfer might be acceptable if a data collecting company has internal rules that are deemed to be adequate. This would enable the flow of information to remain unimpeded. This determination could be funded at the company's expense, as they will

---

[250] Flaherty, above n 37, 229-230.
[251] Lipinski, above n 78. The OECD has recognised that "domestic legislation concerning privacy protection … may hinder informational (data) flows" and has therefore encouraged compatible laws. Discussion Paper No 12, above n 64.
[252] Power, above n 8, 235.
[253] Power, above n 8, 236.
[254] According to Chalton the best the EU can hope to achieve is placing diplomatic pressure on those countries whose information privacy laws are inadequate, above n 46, 7.6

obtain the benefit. The extra cost to the industry should also cause the companies to place pressure on non-signatory governments to become part of the agreement.

D. An Alternative Solution

Harland advocates the development of non-binding guidelines or codes, together with various modes of international cooperation. While these codes would not be legally binding under international law Harland believes they have important consequences and may come to be "soft law". That is they would put considerable pressure on governments and businesses and influence the way business is done. They might also affect the development of legislation, the application of existing law, and the form of government policy.[255] Non-binding guidelines can assist countries in providing a privacy protection framework. They might also stimulate further international cooperation.

The moral force of the guidelines might raise sensitivity over privacy issues.[256] For example, the work of the UN Commission on International Trade Law (UNCITRAL) has been influential in the e-commerce area. UNCITRAL's Model Law on Electronic Commerce (1996) is designed to provide internationally accepted principles on issues regarding paperless communications where there is present uncertainty. This model has influenced Australian and Singaporean legislation.[257] The UN Guidelines also encourage regional cooperation as a way forward, such as via the Asia-Pacific Economic Cooperation, and like that found in the EU.

I believe that due to the potential of the Internet to seriously erode privacy rights what is required is not merely soft law, therefore this option is less preferable to harmonisation. As is clear from the discussion in Part III industry initiatives are insufficient. My view is that effective solutions can only be provided via a legislative system that provides for an adequate enforcement system. This would provide the substantially greater incentives needed to spur self-regulation and ensure widespread implementation of privacy principles.[258]

---

[255] Harland, above n 209, 25-26.
[256] Harland, above n 209, 33-34.
[257] Harland, above n 209, 42.
[258] Martha K Landesberg et al "Federal Trade Commission: report to Congress on privacy online" Part VB3 at <http://www.ftc.gov/reports/privacy3/survey.htm#GeneralSurveyFindings>.

However, it is accepted that a coordinated response could take some time.[259] While major international organisations such as the OECD are in the process of seriously discussing cooperative schemes, for a variety of reasons there are many countries who do not feel the same sense of urgency to combat privacy invasions. This is particularly so for those countries with more pressing social problems to deal with.[260]

The processing of data will tend to migrate to the countries that have the weakest protection.[261] In a financial context experience has shown that when physical location is no longer important, organisations are inclined to move to the jurisdictions that have the most favourable regulatory regimes.[262] Therefore "weak protection" can equate to increased revenue. For example, currently data processors would be more likely to conduct business in the US than the UK that, as noted, has stricter controls in place. This will act as a disincentive, in particular to developing countries. Developing countries are understandably reluctant to endorse guidelines that might restrict industrial development, unless they are offered some guarantee of technological or financial support.[263]

A "soft law" approach, while not a solution, is better than no law and if it is the only available option should be vigorously pursued. As legally binding international standards might be a long way off the development of international standards that are endorsed by Government, industry, and consumers is a way to make progress.[264] Whatever means is ultimately adopted "the world of individual national jurisdictions will need to address the increasingly borderless crimes committed in cyberspace".[265]

VI. FURTHER PROBLEMS

A. Jurisdiction

---

[259] Schamach, above n 204, 64.
[260] Sinrod and Reilly, above n 35, 30.
[261] Chalton, above n 46, 7.6.
[262] Ian W Hutton "Electronic Cash - welcome to the future" (1995) 145 no 6273 New Law Journal 1810.
[263] Harland, above n 209, 37.
[264] Harland, above n 209, 15.
[265] Sinrod, above n 30, 229.

Complicating privacy violation enforcement is the area of legal jurisdiction. As noted global distribution is an inevitable, and central, feature of the Internet.[266] The resulting situation poses a complex jurisdictional question, in the case of a multi-jurisdictional dispute which jurisdiction should the dispute be heard in? A further, and equally complex question, is which law should apply? These issues are not new but these problems are exacerbated on the Internet because more formal and informal relationships can be quickly created across many different jurisdictions. Issues relating to jurisdiction and applicable law were major obstacles for the agreement sought between the EU and the US.[267]

1. Which country has jurisdiction?

With something as ephemeral as the Internet, and because of the transitory nature of websites, it is often hard to determine which country should have jurisdiction.[268] What is required is "an agreement on the cooperation of the enforcement of judgements, so that no state takes (took) exception to an attempt by another state to exert its law of extra-territoriality".[269] Ideally in a harmonised system there would be an international supervisory body that would have jurisdictional competence to govern jurisdictional disputes as to which country has the authority to deal with a complaint.

Even if such a system was agreed to the practical matter of which forum should settle the dispute will still need to be resolved, whether a privacy agency, international body, or court is involved. The extension of one country's jurisdiction to another must have a reasonable legal basis.[270] Therefore an acceptable test will have to be developed. However, the practical effects of this decision would be reduced if the laws in the jurisdictions concerned were substantively similar.

Courts are currently prepared to assert their jurisdiction over those operating in other countries. The following French example illustrates this point. The *Yahoo* case, decided this year, dealt with jurisdiction for the purpose of online auctions. The case

---

[266] Nick Braithwaite "The Internet and Bulletin Board Defamation" (1995) New Law Journal 1216.
[267] Harland, above n 209, 45.
[268] Kirby, above n 195, 117. Michael L Siegel "Online Information Provider Liability for Copyright Infringement: Potential Pitfalls and Solutions" (1999) 4 Virginia Journal of Law and Technology 7, para 9.
[269] Landau, above n 203, 60.
[270] Lipinski, above n 78.

involved a complaint by a French Jewish students group against Yahoo!Inc and Yahoo France. The Yahoo!Inc site contained an online auction site which exhibited for sale more than one thousand items of Nazi memorabilia and hosted the Geocities.com site which had anti-Semitic sites. Yahoo.com itself did not contain the offfensive content but links to sites that contained the material. Yahoo France provided a hypertext link to Yahoo.com.[271]

The court held in relation to Yahoo!Inc that the viewing of illicit content by French websurfers on their computer screens constituted a harm felt in France and that this was sufficient to establish jurisdiction. Jurisdiction was allowed because the activity caused harm to people or organisations in France. This is the first time such meagre grounds have been used to establish jurisdiction. [272]

Clearly an adequate solution must be reached to enable clarity and certainty, as well as reasonable results. Currently tests vary between property, tort, and contract claims. For example, under Article 2 of the Brussels Convention,[273] a plaintiff must issue proceedings against an EC defendant in the courts of the state where the defendant is domiciled. However this rule does not apply to tort in which case the action might be bought against the plaintiff in the place where the harmful event occurred.[274]

There are also many different tests between, and within, different countries. What are some of these different approaches? Firstly, jurisdiction could be restricted to the place where the plaintiff is bringing the action. Consumers International[275] and Japan's Economic Commerce Promotion Council have argued that the consumer's country of residence must be recognised. Another option is the defendant's jurisdiction. Again in the advertising arena the US has advocated the defendant's country of origin rule. This rule has been adopted by the International Chamber of Commerce in its *Revised Guidelines on Advertising and Marketing on the Internet*.[276]

---

[271] Sales Vincent & Associes "Important Rulings on Online Auctions" International Law Office June 29 2000 at <http://www.internationallawoffice.com/ld.cfm?Newsletters_Ref=1924>.
[272] Sales Vincent, above n 271.
[273] On Jurisdiction and the Enforcement and Recognition of Judgements in Civil and Commercial Matters 1968.
[274] Article 5(3) of the Brussels Convention.
[275] Formerly known as the International Organisation of Consumers Unions.
[276] Harland, above n 209, 30.

In America one test that has been adopted is the "totality of contacts" approach. This requires the court to gather and weigh all contacts that the defendant has with the forum, either electronic or non-electronic, to determine whether the contact is sufficient to assert jurisdiction.[277] Furthermore the place where the effects of the action are felt the most might be the appropriate forum. This is another prominent approach in the US.[278] However this "effects doctrine" has not been accepted either by the English courts or the European Court of Justice, although the European Commission has accepted it.[279]

On approach that is not practicable for the Internet context is provided in the EU under the Berne Convention. Following this approach if the harm occurs in more than one place actions may be bought in all those places. Due to potential for a wide distribution of information causing the breach makes it possible for harm, and therefore liability, to arise in various jurisdictions. This would clearly be advantageous to the plaintiff but hugely expensive and cumbersome for the defendant.[280]

The Internet throws all of these standard tests for asserting jurisdiction out of kilter. They are complex and difficult to apply. Judicial responses have been unpredictable.[281] For example, some courts have found that the creation of a website is enough to establish jurisdiction.[282] Others have held that if a passive website invited visitors to contact via e-mail that was sufficient.[283] With differing standards in place, forum shopping will occur. To obtain consistency it might be beneficial to treat the Internet as a special category. While an appropriate test must be formulated I have not attempted to resolve this issue.

2. *Which law should apply?*

If the laws do not conflict, the court will typically apply the substantive law of the forum state. What happens if the laws do conflict? Unless there is complete harmonisation, an outcome that is highly unlikely, this issue is bound to arise.

---

[277] Barry J Waldman "A Unified Approach to Cyber-Libel: defamation on the Internet, a suggested approach" (1999) 6 Rich JL & Tech 6.
[278] Waldman, above n 277.
[279] Landau, above n 203, 60.
[280] Landau, above n 203, 60.
[281] Lipinski, above n 78.
[282] *Inset Systems Inc v Instruction Set, Co 937* F.Supp 161 (1996). *Desktops Techs Inc v Colorworks Reprod & Design Inc*, NO CIV !98-5029, 1999 WL 98572, 4 (ED Pa Feb 25 1999).
[283] *International Star Registry of America v Bowman-Haight Ventures Inc*, No 98 C 6823, 1999 WL 300285 at 607 (ND ILL May 6, 1999).

Following a general tort-based approach, first it must be determined which states have an interest in the application of their law. The court will then have regard to various factors. These are which state has the greatest interest in having its law applied, the relevant policies of the forum, certainty and predictability in the results reached, ease in the application of the law, the promotion of interstate order and policy considerations. Under the traditional multi-state defamation approach the state with the most significant relationship to the conduct will have its law applied, which will usually be the state in which the claimant was domiciled if that was where "publication" occurred.[284]

In the context of defamation Waldman believes the best point to begin is the domicile of the claimant. If the greatest effect of the breach is not in the plaintiff's jurisdiction then a secondary test must apply. This would focus on the location of where the greatest demonstrable injury has been caused, not whether the defendant knew that his or her actions would have an impact in that forum.[285] Whatever approach is adopted the appropriate solution must not be too complex, a contact by contact analysis would take time and money.

B. When should Internet Service Providers be Vicariously Liable?

A further, and equally challenging obstacle, is determining when ISPs should be vicariously liable for the actions of those using their networks. Here we are not concerned with the circumstances in which an ISP should be held liable when they have directly breached an individual's privacy, but when messages or information that are invasive of privacy is posted on its network. Local publication is only possible in an area via an ISP. ISPs are therefore in the best position to monitor abuse and protect the privacy rights of those on the net. Add to this the potential anonymity of the person breaching privacy, and the possible evidential problems of establishing which person sent the information,[286] and it becomes clear that it is necessary to hold ISPs accountable in some situations.

The question is when. For example, should a service provider be liable for the establishment of a link to another web site for violations made on that site? Should the

---

[284] Waldman, above n 277.
[285] Waldman, above n 277.
[286] Braithwaite, above n 266, 1216.

ISP have to review all content on that other site before providing a link, and carry out subsequent checks? Should a provider be liable if they receive actual notice there is a link to an infringing site? Any international agreement would have to deal with this difficult issue.

In the French *Yahoo* case mentioned already Yahoo France was found to have a duty to warn each and every user of the dangers of clicking on a link, despite the infringing information being at least two hypertext links away, to a site that it knows has illicit content. The penalties imposed were unprecedented. Yahoo!Inc had to block access to the illicit sites by French Internet users and also to block all access to incriminated sites. The court held that technical difficulties limiting access to Nazi propaganda on its system were not insurmountable and ordered Yahoo to take all necessary measures to discourage and render impossible any access via Yahoo to auctions of Nazi memorabilia.[287] Is this an appropriate result?

I would argue it is not, due to the vast amount of information placed on the network daily and the ability of users to place information on, for example, bulletin boards. Service providers have far less opportunity than traditional information providers to review content.[288] If strict liability were enforced then censorship in the form of monitoring transmissions would occur.[289] Additionally it is usually not immediately apparent to the provider that any privacy laws have been breached, unless a complaint is received.

The amount of control an ISP has over the information should be made determinative. At one end of the scale is where the provider determines the content of the messages and disseminates them, at the other end is the provider of a bulletin board for the private distribution of information.[290] This is the approach taken in the defamation context which provides various "innocent dissemination" defences to try and limit ISP liability.

In Britain, under the Defamation Act 1996, those with only secondary responsibility for the publication of defamatory material (including ISPs) escape liability if they are not

---

[287] Sales Vincent, above n 271.
[288] Davies, above n 3, 10.
[289] These arguments were noted in relation to copyright infringement but are equally applicable to breaches of privacy. Irina Y Dmitrieva "I Know it When I See it: should Internet Providers recognize copyright violation when they see it?" (May, 2000) 16 Computer & High Tech LJ 233, 237-8.
[290] Bartlett, above n 139, 111.

the author, editor, or publisher of the allegation. This would not protect an ISP who deliberately published the information.[291] Similarly in New Zealand a recent Law Commission report has suggested that an ISP should only be liable for republishing defamatory statements if it had actual knowledge of the material, and therefore control.[292] The current NZ Defamation Act provides a defence to distributors, but the application of this to ISPs has yet to be tested in court.

It has been argued that introducing such a knowledge or control requirement encourages providers to turn a blind eye to privacy violations and to refrain from offering any form of control. Despite this criticism it seems reasonable that if having taken all reasonable care an ISP did not know, or have reason to know, the information was breaching privacy then liability should not be incurred. If they were required to control or have knowledge of Internet content this would not only increase legal risks but also increase the cost of supervision which could stunt the growth of the information superhighway.[293]

A good approach to ISP liability that should be adapted for the privacy protection context is provided in the Online Copyright Infringement Liability Limitation Act 1998 (OCILLA) US. Under this Act service providers are not liable for most forms of relief for copyright violations if they fall into a number of safe harbours. If the ISP is carrying out certain passive functions liability is limited.[294] Graduated liability is provided as ISP involvement increases. To be eligible for liability limitations the ISP must designate an agent to receive notification[295] of copyright violations and must implement a policy for the termination of accounts of subscribers who repeatedly violate copyright.

An ISP must also remove material that is claimed to be infringing upon notification from the copyright owner. Once notification is received the ISP must take down the allegedly infringing information. This would help avoid situations arising like those in the Demon case. Earlier this year Demon Internet paid more than £230,000 in damages

---

[291] Amber Melville-Brown et al "Reform at Last in Defamation Law after Centuries of Little Change, and Points of Future Trends" (2000) 97(7) Law Society's Gazette 24.
[292] Bell Gully, above n 162.
[293] Angel, above n 24, 113.
[294] Under this definition they must not initiate, select or modify communication content, determine the message recipients or retain a copy on a system or network longer than is necessary for the transmission if that system or network is ordinarily accessible to other people. Remaining passive includes the mere provision of e-mail services, newsgroups, and listserv services. s512(a)(1-5).
[295] The requirements and procedures for notification are provided for in section 512.

and fees to end a court action by an academic, Laurence Godfrey, who said he was defamed by two anonymous Internet postings. Godfrey had asked the ISP to remove the posting but the ISP refused.[296] The statute also allows for counter-notification, to allow for fairness and balance. A user can argue, under the threat of perjury, that the material was removed due to a mistake or a misidentification.[297]

The purpose of the Act is to provide certainty and enforcement but also to allow for the development of networks and avoid censorship. Copyright owners are given primary responsibility for the enforcement of their rights because they are in the best position to make well-informed judgments as to what constitutes a violation. This is the same for privacy. Generally, only the individual involved will know whether the information was consented to or was used in breach of privacy.[298] This approach seems to effectively balance the need for ISP's to take responsibility for information that breaches the principles while ensuring that internet growth is not stunted or that censorship does not occur.

What must be avoided is an approach that unfairly favours either the ISP or the claimant. For example, a complete shield from an action unless the service was the actual author of the content should not be implemented. Such an approach was adopted in the defamation context in the US in the Communications Decency Act 1996. [299] Under this Act even contract employees of service providers have been held to be third parties thereby removing the ISP from the equation. Liability is only incurred if a person is a direct employee of the ISP .[300] The effect has been to protect ISPs from liability even where they retain editorial control. This removes the incentives for ensuring that offending material is not disseminated or is promptly removed. Innocent parties might be without compensation.[301]

---

[296] Patrick Barkham "Internet Regulation 'a threat to civil liberties' GuardianUnlimited Special Report May 3 2000 at <http://www.guardianunlimited.co.uk/freespeech/article/0,2763,216809,00.html>.

[297] Dmitrieva, above n 289.

[298] Dmitrieva, above n 289, 261.

[299] The Act provides that "no provider or user of any interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". 230(c)(2)(A)-(B)

[300] Matt Drudge published a report via e-mail and received a flat monthly $3000 fee for providing his publication to AOL customers. AOL reserved the right to modify the content of the report. Drudge printed defamatory information about a man claiming he had a history of domestic violence against his wife. This connection was not held sufficient to remove Drudge from the third party category.

The problem with this has been made blatantly obvious by the Kenneth Zeran case.[302] A posting on an AOL bulletin board advertised that Zeran was selling T-shirts that were making jest at the Oklahoma City Federal Building Bombing – as a result he received angry and derogatory calls as well as death threats. Zeran bought a defamation action after he claimed AOL had taken an unreasonable time to remove defamatory messages and failure to post a retraction after Zeran had notified the provider of their existence. The court held that ISPs were not liable for information originating from third parties and failure to exercise "editorial control" was not a basis for recovery, thereby limiting Zeran's claim to the original author.

Piercing anonymity

In order to bring an action for breach of privacy against a user it is sometimes necessary for ISPs to disclose the identity of the user or to trace their activities. Contrary to popular belief even where individuals take privacy precautions it is generally possible to establish where the information originated from by means of the IP address.[303] Unfortunately, obtaining such information can itself be a breach of an individual's privacy. Reflecting on the example at the start of the paper, McVeigh had his privacy breached when AOL identified him, despite the Navy remaining unidentified and not possessing a warrant. Last year a Canadian Court ruled that ISPs can be ordered to reveal the identity of their users, despite the fact that the service providers had not been joined in the proceedings.[304]

The international agreement must explicitly outline situations in which such information may be obtained and it must provide procedural safeguards.[305] In the US the Electronic

---

[301] Waldman, above n 277.

[302] *Zeran v America Online Inc* 129 F3d 327 (4th Cir 1997).

[303] Without an IP address it is not possible to connect to any computer on the Internet. Technically the IP address could be avoided by the use of "spoofing" or by means of a proxy server but this is difficult and out of the reach of the usual user. The address will almost always provide the organisation where Internet access was achieved and the ISP will probably have a log that can identify the individual user and the date and time of contact. Sobel, above n 157, footnote 12.

[304] Harbottle & Lewis Solicitors "Internet Service Providers can be Called to Identify Users" (1999) 4(1) Communications Law 31.

[305] Sobel provides an example of appropriate safeguards that should be followed before information can be released: there should be the presentation of a subpoena; in civil cases the user should be informed and given a reasonable amount of time to take action (such as a move to quash); if the matter is taken to the court Sobel has identified various factors that should be considered such as specificity of notice and previous attempts to locate the defendant. Sobel, above n 157, paras 19 - 21.

Communications Privacy Act requires law enforcement agencies to obtain a judicial issuance of a warrant, subject to specific procedural requirements. For civil discovery, however, the statute is permissive and allows the provider to disclose the record.[306] However, again the approach favoured is that provided for in the OCILLA. Under this Act the copyright owner can request a federal district court to issue a subpoena to an SP for identification of the alleged infringer. If successful the ISP must provide all personally identifying information in its possession.[307]

This information should be included in websites privacy policies so that users are aware of the potential for them to be identified. By opting in to the service the user would consent to this identification in appropriate circumstances. This would protect privacy but also provide an incentive for individuals to follow privacy laws, due to the potential for them to be identified and might become the subject of an action.

VII. ENFORCEMENT: A PROPOSAL

Regardless of whether harmonisation has occurred national legislation should be implemented providing for adequate privacy principles and an effective enforcement system. If there is a harmonised agreement this national legislation should at least implement the internationally agreed minimum principles. More stringent principles could be added by nations if they chose. For example, the government might impose a duty to build privacy protection features into technological designs.[308]

How should the general principles of the international agreement, and national legislation that implements it, be enforced? Such general principles must by necessity be ambiguous and it is impossible to reconcile conflicts by legislative language.[309] Supervisory bodies must therefore carry out this reconciliation on a case by case basis. This allows for the flexibility that is necessary both to protect the privacy of individuals and to promote the growth of the Internet as an information provider and avenue for e-commerce. Such an approach is appropriate as it can accommodate new technologies or problems that are yet to surface.

---

[306] The statute provides that a service provider "may disclose a record or other information pertaining to a subscriber .. to any person other than a government entity" 18 USC 2703 (c)(1)(A).
[307] Dmitrieva, above n 289.
[308] The recommended Canadian Charter of privacy rights includes this principle.
[309] Rigaux, in Aldhouse, above n 7, 12.

These principles in conjunction with effective enforcement give the user increased control over his or her information. What users need is practical and available protection for their informational privacy.[310] They need a cheap, quick and effective solution that can resolve the majority of claims. Any claim would first be made to the industry. If a satisfactory resolution is not reached in appropriate circumstances a privacy agency would hear the case. Finally, an appeal may be made to a tribunal or court. Under the classification system previously mentioned this proposal could be described as a passive scheme with enhanced enforcement capabilities.

A. The Industry's Role

While a workable solution must be adopted there is no clear cut choice between self-regulation or government control via legislation; both are required.[311] Industry involvement is required primarily to reduce costs. Any solution must have industry support or enforcement would be extremely expensive and the laws would be impossible to police. What must be borne in mind is the "general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way".[312]

Any form of regulation will probably therefore emphasise industry-generated codes of conduct. The use of such codes has become increasingly acceptable. The Privacy Commissioner should issue or endorse Codes of Practice for particular groups or services. Allowing for the development of effective and broadly applicable codes would allow for flexibility, broad coverage, and industry involvement. These codes may be modified for specific industries to make them more or less stringent. As far as possible these modified codes should implement the same basic principles. In appropriate cases modified codes remove procedural complications and can avoid significantly increased costs.[313] Provisions could be tailored to meet existing conditions, this is particularly important in a highly technological and constantly changing industry. The use of differing codes should, however, be used sparingly to avoid both user and collector confusion and make compliance easier.

---

[310] Reilly, above n 6, para 147.
[311] Valentine, above n 68.
[312] Privacy Act 1993, s14(a).

Any code of practice must comply with the following principles provided by the OECD. A successful code of practice should: contain positive statements providing a commitment to data protection principles ("form"); be tailored to the industry or company, not merely state general principles, and attempt to apply the principles so they are workable ("substance"); deal with the data protection issues specifically confronting the relevant industry/company ("level of detail"); be written in simple readily comprehensible language for those in the relevant industry ("transparency"); provide for an implementation procedure within the industry to provide certainty, this could include privacy officers who are responsible for privacy issues and report to management ("implementation"); provide for occasional review to assess relevance and make changes if necessary ("review"); be underpinned with a means of control or enforcement whether legislative, contractual or administrative – there must be a means of redress for data subjects or other interested parties ("control").[314]

The data collectors should then implement individual policies with the code as a baseline and default provision. This development of internal guidelines is important.[315] Appropriate industry schemes could be approved by the Commissioner, such as TRUSTe or BBB. A breach of the approved scheme would be considered a breach of the relevant privacy principles. The industry should bear the cost of this approval as they will be receiving the benefit from such a system. These schemes should provide their own enforcement mechanism. The Commissioner would therefore have no direct role in enforcement unless the decision reached, sanction imposed, or remedy awarded was unfair.

As an incentive to market compliance, other than sanctions, businesses could be shielded from litigation as long as they comply with the privacy code or approved schemes. If they could not be shielded at least it could be guaranteed that this would be a strong consideration in the commissioner or court's decision. Currently industry initiatives do not shield data collectors from liability. There is evidence to suggest that traditional legal precedent will override Internet customs or self-regulating practices.

The goal of privacy protection and legislation should partly be self-regulation. The focus should be on Governments in partnership with business and other relevant sectors

---

[313] Evans, above n 169, 185.
[314] Tucker, above n 59, 67.
[315] Tucker, above n 59, 81.

of society to develop and implement strategies. The user should therefore generally be required to complain to the industry or appropriate sanctioned scheme agency concerned first about any action that is, or appears to be, privacy interference.

B. The Privacy Agency

If the individual is not satisfied with the industry provided response an effective avenue of complaint must be available. An external mechanism must be in place to receive complaints and to analyse and act upon them. This independent body can also act as a contact point with other jurisdictions, and cooperate in the investigation of complaints.[316] The agency's decisions would be seen as more legitimate to the public and the presence of an independent enforcement mechanism would increase consumer confidence. The publication of decisions would help provide guidance for how the industry should be acting.

The approach favoured is the establishment of, or use of an existing, privacy agency. Using institutions already in place would reduce start up costs and allow for a type of intervention that has already been found to be effective. One extremely viable option is that of the privacy commissioner model, which is flourishing worldwide. Canada created this system which has been enthusiastically adopted by many countries. For example, New Zealand has followed this model as have all of the EU countries that have the equivalent with their Data Protection Commissioners.[317] Such agencies typically provide a low-cost, or possibly no-cost, forum for resolution. The agency should adopt an investigative and non-adversarial model using mediation to resolve disputes. This leads to a much simpler process and speedier resolution than that provided by a court, and offers a less formal setting. The further disclosure of personal details of investigations can be avoided. These factors make an agency more accessible to the public.[318]

In New Zealand, experience has shown that few people are unhappy with outcomes reached by the Privacy Commissioner. In fact many agencies are on good terms with the Privacy Office and cooperate with investigations. Such a situation should be the

---

[316] This is the view of Professor Rigaux, "La vie privee, une liberte parmi les autres", paper presented at the 19th International Conference of Privacy and Data Protection Commissioners, Brussels, 17-19 September, 1997 as noted in Aldhouse, above n 7, 12.
[317] Flaherty, above n 37, 223.
[318] Evans, above n 169, 171.

aim of the agency. As noted the support of the industry will lead to a cheaper and more effective system[319]

1. Procedure

Recourse to the agency should be available if one of the provisions in the applicable code of practice, industry scheme, or legislation was breached and the data collector or sanctioned enforcement agency has not taken appropriate action. As with the current system in New Zealand, the agency could refuse to take action on appropriate grounds. That is, if the complaint was trivial, the complainant had unreasonably failed to follow a complaints procedure provided for in a code of practice, or where there is another adequate remedy, particularly that provided by the industry itself.

If a user has complained to a company that is part of a sanctioned scheme, such as TRUSTe or BBB, and that enforcement agency has investigated the complaint the agency should not normally become involved. This is particularly so if a remedy has already been provided or a sanction has been imposed. In such cases the aggrieved party could still choose to issue his or her own proceedings in a court.[320]

If the agency believes the complaint has substance best endeavours should be used to ensure a settlement and a satisfactory assurance against repetition. In England the Data Protection Commissioner can assist or take over the case of individuals who want to enforce their rights against the media but only if the case has significant public importance.[321] A similar approach could be adopted with important violations of any of the informational privacy principles.

The Commissioner should also have the power to act independently of any complaint and the ability to inquire generally into any matter, including any law, practice, or procedure in the private or public sector.[322] This is particularly important as Internet privacy beaches are not necessarily readily apparent to the individual concerned. In a case of group harm, with little or no individual harm, it is likely that the Privacy Commissioner itself will need to act on its own without a complaint. Without individual

---

[319] Evans, above n 169, 171.
[320] Discussion Paper No 3, above n 225.
[321] Rasaiah, above n 181, 185.
[322] Privacy Commissioner *A Guide to the Privacy Act 1993 - Fact Sheet No 1* (Wellington, 1 July 1993).

harm it is unlikely that an individual will be prepared to take the time and effort to complain.

The Privacy Rights Clearinghouse model could be utilised as an avenue for consumer complaints, particularly by those who do not wish to take the matter up on a formal level.[323] Initially a toll free hotline was set up which fielded approximately 10,000 calls per year from consumers that were handled by the director of the Clearinghouse and law students. Due to funding cuts the service was discontinued. A website has now been established and e-mail is used to receive approximately three to four thousand messages a year. The information learned is reported to legislators, regulators, government officials, industry representatives and other consumer advocates.[324] If enough complaints are received then the agency could initiate its own investigation. This model would also allow for direct interaction with consumers and thereby enables the agency's educative function to be fulfilled.

Another approach that could be adapted for the privacy context is that used by the Internet Watch Foundation. This government-supported organisation assesses the legality of pornography that is reported by the public via a hotline. It then notifies the service provider concerned and the police about any potential breaches and can implement takedown procedures to remove content regarded as illegal.[325] The hotline has been used as a model in Europe, the US and Australia.[326] However, it should be noted that the foundation has been criticised as it is not a public body and is neither accountable nor transparent.[327]

2. Remedies

Whatever agency is used it must have real powers to be effective. If a claimant is harmed a remedy should be provided to that individual. As with the Directive compensation should be available in appropriate circumstances to cover damage and distress[328], and for loss or unauthorised disclosure.[329] However, damages are not the only option. Other options include a compulsory internal administrative review or

---

[323] The Privacy Rights Clearinghouse is a Californian institute that was established in 1992. Its mission is to increase Californian's awareness of how technology is affecting their lives as well as giving them practical information on how to safeguard their privacy.
[324] Givens, above n 9, 347.
[325] Barkham, above n 296.
[326] Kerr, above n 249.
[327] Yaman Akdneiz "Copyright and the Internet" (1999) 147 (6798) New Law Journal 965.
[328] Privacy Act 1993, s22(1) (NZ).

mediation process.[330] Various forms of redress should be provided including, informal complaint resolution, mediation, arbitration and civil litigation,[331] periodic compliance audits (paid for by the wrongdoer), and neutral complaint investigation.[332] Furthermore the agency could impose cancellation of the right to use a certifying seal or post the name of the non-complier on a "bad actor" list.[333]

There should not necessarily be a requirement for damage, or significant humiliation or injury to feelings to an individual before a sanction is imposed. Often a breach of informational privacy principles results in only a minimal loss to an individual but to a group may cause damage. Further while the breach may appear trivial at the current point in time in addition with other information collected it could become significant. If no harm to an individual claimant is caused but practices are held to breach privacy principles the offender should be made to implement new practices to avoid future breaches or made to undergo and audit. Even without harm individuals should have rights to correction or erasure of inaccurate data.[334]

The aim should be purely to redress damage but to deter future breaches. In appropriate cases, therefore, fines up to a specified maximum limit might be imposed. These fines should, however, be rarely used and only to punish those that blatantly disregard users' privacy. A pragmatic approach must be adopted that relates to the harm caused to an individual or a group.

3. Funding

Funding could pose a significant obstacle to the effective implementation of the scheme. Without adequate funding the system will not succeed. In New Zealand there are already long delays resolving privacy claims due to "substantial under-resourcing". This reduces the accessibility of the agency and undermines the whole system.[335] This problem would be exacerbated if Internet complaints were added to the agency's ambit without the provision of extra funding.

---

[329] Privacy Act 1993, s23 (NZ).
[330] Valentine, above n 68, 407.
[331] These are the measures advocated by the Privacy Working Group, noted in Belgum, above n10 , n115-117.
[332] Valentine, above n 68, 407.
[333] These are the measures advocated by the Privacy Working Group, noted in Belgum, above n10, n115-117.
[334] Privacy Act 1993, s 24 (NZ).

Currently the Privacy Commissioner model is state-funded. As many of the Internet privacy violations are caused by the private sector it makes sense that the cost should to some extent be borne by that sector. Non-compliers should pay the cost of assessing their non-compliance. It is reasonable to impose costs on those agencies that cause the harm and, more often than not, profit from the violations.

Private sector funding might, however, taint the independence of the Commission. The fear is that this could provide an incentive to the agency to allow claims and find a data collector to have breached the principles. However, if the only benefit is that the cost of the assessment is recouped then the Commission will not profit from bringing charges. Further, there is a right of appeal to a tribunal or court who could overturn an unfair ruling.

Furthermore there is currently no suggestion that the income source has dictated the outcome of the complaints process With government funding there was the fear that the government could control outcomes by, for example, not bringing charges against government departments. This fear turned out to be unfounded.[336]

As noted the emphasis placed on self-regulatory initiatives and industry resolution should reduce costs. If a collector has made all reasonable efforts to resolve the case this should be a major factor in determining whether the claimant has a viable claim. The parties should be encouraged to work out a result amongst themselves, with the threat of sanctions as an incentive.

The Commission's effectiveness would be enhanced if, as in Canada, it could undertake audits on reasonable notice if the Commissioner has reasonable grounds to believe the organisation is contravening a provision or not following a recommendation.[337] In New Zealand the Commissioner also has the power to audit agencies, but has not done so due to the cost. Without significant funding the Commissioner could only carry out his function if the agencies had to bear the cost themselves.

Either mandatory audits could be implemented, paid for by the organisation, or sufficient incentives must be in place for the voluntary undertaking of such audits.

---

[335] Evans, above n 169.
[336] Evans, above n 169, 186.
[337] Power, above n 8, 241.

Incentives such as priority for government assignments and increased public confidence, particularly if accompanied by a publicity drive, might lead to some companies agreeing to audits. These incentives could also be used to entice companies to join sanctioned industry schemes. Those that pass an audit, or those that are part of a sanctioned scheme, could be given the Privacy Commissioner's own "seal of approval". A seal issued by the Privacy agency would provide clear and certain assistance to users.

4. Educational role

Apart from the establishment of a complaints procedure consumer education is necessary. This function would largely fall on the shoulders of the agency. Website privacy policies are inadequate information providers as they are often hard to locate and to understand. Most users are unaware of the potential privacy impacts of the relinquishment of their information, what information is being collected, what it may be used for and what rights they have. Education allows for informed decisions about, for example, what information to release and what sites to visit. If customers learnt to enhance their own privacy this would be the cheapest and most efficient form of protection.

The Commissioner should embark on an educational campaign, via such means as websites, television and radio advertising, and pamphlets. Information should be provided on users' legal rights, means of redress and the best means of protecting themselves from privacy breaches. This would include information about technologies that can safeguard users' privacy, such as encryption and anonymisers,[338] because it will still be hard to practically enforce data protection legislation.[339] Potentially a list of those who fail to comply with privacy rules could be published. These measures should spurn self-regulation as customers become more aware of the privacy risks. The Commissioner should also work to educate data collectors to prevent future damage and improve practices.

Ideally the agency would also identify areas where there is a major potential for privacy breaches and suggest solutions. It would take a proactive role by looking at the privacy interests in new Internet technologies.[340]

---

[338] Givens, above n 9, 355.
[339] Noeding, above n 32, 91.

C. The Courts

Finally the applicant or data collector should be able to apply to another tribunal or to a court for a hearing, which should be able to award damages, order correction of the offender's practices or overturn a decision of the agency.[341] Again for serious breaches fines might be imposed, which might then be used to fund the system.

In New Zealand the principles are generally not directly enforceable in court.[342] The courts should be freed to explicitly recognise privacy rights and enforce the principles adequately. This is necessary to try and address the lack of a strong history of privacy litigation success that is apparent in New Zealand, Australia, Canada, England and America.[343]

In England at any time prior to the time when the defence is served a publisher (ISP) can make a written offer to the claimant and resolve the matter outside of the courts. This is attractive for both parties as if the offer is accepted it would provide speedy resolution and involve fewer costs.[344]

The problems involved in court resolution explained above must be borne in mind. Therefore ideally most complaints should be resolved via the internal mechanisms or the agency. Previous measures of attempted resolution by both parties should be an integral part in determining appropriate remedies. There must be measures in place to ensure that trivial litigation is discouraged.

D. The Government: a special case?

These data protection initiatives must apply to both the private and the public sector to be effective[345] as both hold large amounts of personal information. Perhaps no boundary should be recognised in the flow of information between the two so that

---

[340] This is one of the roles adopted by the Privacy Commissioner in the Canadian system. Flaherty, above n 37, 228.
[341] Power, above n 8, 241.
[342] Evans, above n 169, 197.
[343] Flaherty, above n 37, 221.
[344] Melville-Brown, above n 291.
[345] As in the OECD guidelines New Zealand makes no such distinction. Canada's Bill C-6 would protect information in the private sector and require compliance with a wide range of fair information practices already applicable to the public sector.

loopholes and demarcation disputes do not arise.[346] The public-private distinction can be highly artificial, particularly with "privatisation, contracting out and outsourcing of formerly government functions. In information terms, no boundary is recognised in the flow of data between the public and private sectors".[347] However, different considerations may arise that might warrant the development of different codes.

The Government itself, or through private companies, might obtain information off the Internet. It might also place personal information onto the Internet, or sell it to third companies who will. The Government's collection and use of information is, however, different to that of the private sector as often individuals have no choice but to disclose their personal data. After collection the information subject normally lacks the authority to prevent the government from disclosing such information. Even information disclosed for express and legitimate purposes might be resold or used for secondary and unapproved purposes, such as data matching. However, unlike private industry the government has "legitimate interests for engaging in non-consensual uses of personal data that outweigh the privacy interests of individuals whose personal data might be shared". Privacy interests of individuals must often give way to the wider goals of public administration.[348] This however, might be partially addressed via specific "information matching" programmes.[349] Furthermore specific Public Register Privacy Principles could also be enacted.[350]

Another important consideration is that maximum access to government information is regarded as a fundamental right and delay or denial of access has been seen as censorship [351] and might be contrary to Official Information Acts. Freely available information can be seen as providing constitutional safeguards by allowing individuals to determine how decisions were made and giving the opportunity to challenge the validity of those decisions.[352] It is arguable that all non-exempt records should be posted on the Internet, provided that sufficient procedural safeguards are put in place to make sure the information is current and accurate.

---

[346] Privacy Commission *Compliance and Administration Costs – Discussion Paper No 1* (Auckland, 1997).
[347] Discussion Paper No 9, above n 346, 9.
[348] Thumma and Jackson, above n , .
[349] These programs are allowed in NZ under the Privacy Act 1993. Privacy Commissioner *The Privacy Commissioner – Fact Sheet No 2* (Auckland, J July 1993).
[350] These are also provided for in the NZ Privacy Act 1993. Fact Sheet no 1, above n 322.
[351] Paul McMasters "Censorship at the Source: the worst kind" The Freedom Forum Online, 5 February 2000 at <http://www.freedomforum.org/news/2000/05/2000-050-2-06.asp>.
[352] Evans, above n 169, 24.

For these reasons explicit guidelines are required as to the way data may be shared amongst government agencies or the situations in which it may be released to the public via the Internet or onsold to companies who may do the same.[353]

[353] Thumma and Jackson, above n 158.

VIII. CONCLUSION

If some degree of certainty about data information principles can be provided data subjects and data providers will be able to ascertain their opportunities and their responsibilities in regards to the use of information. However whatever system is in place it must be flexible enough to adapt to the ever-changing Internet environment. By 2004 it has been predicted that the Internet will be a "Wireless World" with a majority of Internet participants accessing the Internet via mobile terminals.[354]. There is no point implementing a system that will be obsolete within a short span of time. Using broad principles on an international and national level allows legislation to weather the storm of technological change. The codes advocated provide the flexibility and the focus required to deal with this rapidly changing environment.

It will inevitably be argued that this system will pose a threat to freedom of expression. It is not doubted that the Internet has the ability to enhance freedom of speech. However, the American view that freedom of expression and privacy inherently conflict is incorrect. If there are adequate protections available for the privacy of individuals they will be more likely to freely express their ideas. Conversely the more individuals lack the ability to control their information the less likely they are to impart information.[355] Lack of privacy protection will lead to caution and self-censorship.[356] It is accepted that their are limits to privacy, not only to the extent that an individual puts him or herself into the public arena but also, for such activities as law enforcement, media, national security or freedom of information requests, or on public interest grounds.[357] These exceptions would have to be part of any privacy code or protection.

The threat to civil liberties and e-commerce is that "if governments do not find workable ways of policing the Internet by reasonable and cooperative means and they fall back on the more traditional and oppressive authoritarian styles of regulation".[358] An example of the danger of strict laws was provided in Britain where lawyers have

---

[354] The ARC Group "Wireless Internet: applications, technology and player strategy" (1999) at <http://www.the-arc-group.com/reports/wireless<uscore>internet/toc<uscore.wi/htm>.
[355] Aldhouse, above n 7, 11.
[356] Belgum, above n 10.
[357] This is noted in Strasbourg jurisprudence, see Andrew Drzemczewski "The right to respect for private and family life, home and correspondence" Human Rights Fils No 7, Council of Europe, Strasbourg, 1984.
[358] Kerr, above n 249.

used the threat of prosecution[359] to remove websites from servers. Such a heavy-handed approach must be avoided, what is required is workable co-regulation[360] backed up by legislative sanctions.

[359] Under Britain's 1996 Defamation Act and stringent libel laws.
[360] This is the view of David Kerr, chief executive of the Internet Watch Foundation. In Barkham, above n 296.